DEVELOPING RISK PROFILE ON A ROLE LEVEL

BROCHURE RISK-SENSITIVE ROLES APPENDIX

EXAMPLE: WORK AREAS (BOLD), DUTIES AND POWERS

Granting/awarding

- Issuing access passes to company premises
- Managing authorisations
- Granting authorisations for company software

Collection/receipt

- Receiving payments from customers for products or services supplied
- Collecting invoice payments
- Receipt of fundraising proceeds and donations (by non-profit organisations)
- Levying and collecting taxes
- Collecting membership fees in a membership organisation
- Receiving investments or grants
- Receiving goods and services from suppliers upon delivery

Expenditure, outsourcing, procurement

- Purchasing goods such as office supplies, software licences, marketing services or machinery
- Placing orders with and awarding contracts to suppliers
- Hiring consultants or freelancers
- Outsourcing IT management to an external party
- Awarding a contract to a supplier following a tender
- Outsourcing logistics to a transport company

Payouts/awards

- Awarding year-end bonuses to employees
- Granting subsidies to partners or charities
- Allocating a company car or training budget to an employee
- Paying out sales bonuses

Assessment

- Holding performance reviews with employees
- Assessing suppliers on delivery reliability and value for money
- Selecting and assessing applicants during recruitment procedures
- Assessing audit results relating to internal processes

Enforcement

- Conducting internal checks on compliance with safety regulations
- Enforcing GDPR requirements
- Imposing sanctions for breaches of codes of conduct
- Checking expense claims
- Taking disciplinary action in response to misuse of company resources
- Imposing fines

Handling information

- Handling sensitive or confidential information
- Managing confidential customer data in a CRM system
- Responsible use of company laptops and work phones containing sensitive information
- Data processing

Handling resources

- Appropriate use of a company car and fuel card
- Managing expenses and monitoring budgets within projects or departments
- Accurate expense claims
- No inappropriate use of work equipment such as laptops, work mobile phones or internet access

Third-party contacts

- Contacts with competitors, customers, suppliers and foreign parties, such as in negotiations with suppliers on prices and contract terms
- Working together with international partners in joint ventures
- Customer contact during aftersales or customer service
- Discussions with industry peers in a professional association or at networking events
- National en international parties that approach you

EXAMPLE: VULNERABILITIES

Autonomy/working alone

- A high degree of discretionary power
- Often making decisions and carrying out work alone
- Frequently working from home or other remote work

Specialist/key role

- Being the only person with specialist knowledge
- Concentration of knowledge in one person or a small group
- Working alone in a crucial or process-critical area

Employee's personality traits and situation

- Gambling addiction or other addiction
- Financial problems
- Lack of career prospects
- Criminal contacts
- Feeling unfairly treated
- Attaching great importance to power and status
- Certain convictions

Revolving-door arrangements/conflicts of interest

- Employees who have an ancillary position that closely relates to their role in the organisation
- Former or current employees who are rehired as consultants or engaged as suppliers

Management/leadership

- Management attitude and modelling behaviour
- Tone at the top

Organisational culture

- Competitiveness
- Unrealistic expectations
- Culture of fear
- Different cultures existing alongside one another
- Tight deadlines
- Pressure resulting from stock exchange listing
- Competitive pressure
- Inadequate behavioural modelling in the immediate environment, such as from colleagues

Complexity

- Complex legal or tax structures
- Unclear partnerships
- Opaque production or supply chain

Change/dynamics

- Strong growth or contraction
- Crisis situations
- Budget cuts/reorganisation
- Organisational change such as a merger, acquisition, relocation, etc.
- Use of new technologies such as AI

EXAMPLE: MEASURES

Granting/awarding

- Authorisation policy based on role or function (need-to-access)
- Registration and approval of each access pass by an authorised manager or HR
- Automatic deactivation when employment ends or after a long period of inactivity
- Access logs and records of movements within sensitive areas
- Restricted access to critical areas, such as server rooms and archives
- Two-factor authentication for sensitive access, such as a pass with PIN code or biometrics
- Rights per role, function or process
- Authorisation request procedure with approval by the responsible manager and system administrator
- Ensuring that money is received digitally
- Automatic link between invoicing and accounting systems
- Use of unique payment references, such as a structured payment reference
- Training staff on tax regulations
- Segregation of duties, for example between ordering and approval
- Periodic review of access rights, for example quarterly
- Logging and monitoring of critical actions in the system
- Immediate revocation of access in the event of a change of role or function or departure
- Documented and signed powers of attorney/authorisation lists
- Authorisation matrix linked to roles/functions, amounts and processes. Two-signature principle for higher amounts or high-risk decisions.
- Management of powers of attorney in a central register, with annual checks
- Restrictions in banking or software systems that allow only authorised actions
- Use of recognised payment channels, such as iDEAL, SEPA or credit card with 2FA
- Transparent donation register linked to bank statements
- Transparent reporting and objection procedures

EXAMPLE: MEASURES – CONTINUED

Collection/receipt

- Restricting access to account information (authorisation management)
- Daily reconciliation of payments with outstanding invoices
- Setting out and monitoring clear grant conditions
- Segregation of duties in applying for and registering grants
- Prior approval by authorised persons
- Internal checks comparing grant applications with amounts received
- Periodic checks by an independent internal or external auditor
- Use of validated calculation models/software
- Checking active membership status before collection

Expenditure, outsourcing, procurement

- Setting up red flags in the payment system for unusual transactions
- Written declaration of interests to prevent conflicts of interest
- Budget check before ordering (approval workflow)
- Use of an authorised supplier list
- Procedure for opening quotations with several employees present
- Segregation of duties between applicant, approver and recipient
- Checking the purchase order against delivery note and invoice
- Comparison of quotations for purchases above a threshold amount
- Registration of orders in a central system
- Formal ordering procedure mandatory for all purchases
- Authorisation matrix for approving orders
- Transparent supplier selection and documented rationale
- Checking for duplicate orders via order history
- Clear SLAs (Service Level Agreements) with measurable KPIs
- Security clauses and privacy clauses in contracts
- Use of framework agreements where possible

Payouts/awards

- Clear policy rules and criteria laid down in the collective labour agreement, employment regulations or policy
- Automatic calculation via the payroll system, linked to HR data
- Approval by HR or management before payment
- Segregation of duties between calculation, approval and payment
- Transparent bonus structure based on measurable and verified performance
- Checks by management or finance before approval
- Publication of annual reports on the use of funds
- Restricted access to donation management
- Reconciliation between order, delivery note and invoice
- Goods receipt checks, both qualitative and quantitative
- Use of order forms and receipt forms
- Only authorised suppliers may be in the system
- Annual review and approval of membership fees
- Automatic invoicing and collection linked to membership management
- Member portal for viewing membership status and payments
- Screening employees for possible risks

- Regular evaluation and audit of the IT supplier or other suppliers
- Restricting access to critical systems (principle of least privilege)
- Escrow arrangements for software and code in the event of bankruptcy
- Drawing up clear assignment descriptions and deliverables
- Comparing rates with market standards or benchmarks
- Limiting contract duration and expenditure unless renewed
- Prior approval by the authorised manager/director
- Checking for dual employment or conflicts of interest
- Strict compliance with procurement legislation (public, private/invitational, EU thresholds, etc.)
- Transparent assessment criteria announced in advance
- Multi-member assessment committee
- Information barriers between tenderers and decision-makers
- Documentation and archiving of the entire process
- Track-and-trace systems to monitor deliveries

- Assessment by an independent committee, rather than one person
- Company car policy with clear allocation conditions, such as job level, mileage allowance and private use
- Checking invoices and proof of participation/certificate
- Grant agreement with performance or reporting obligations
- Formal application procedure with documentation requirements
- Approval procedure involving HR or the fleet manager

EXAMPLE: MEASURES – CONTINUED

Payouts/awards – continued

- Spot checks for accuracy and completeness
- Recording bonuses in written agreements
- Checking for duplicate or incorrect awards through payroll processing
- Recording the bonus calculation and supporting rationale in the file
- Checking the recipient's legal status, reliability and use of funds
- Follow-up via a learning portal or HR tool
- Including a training or repayment clause for more expensive courses
- Screening employees for possible risks
- Use of standard contracts stating rights and obligations
- Registration in the HR system linked to the payslip/payroll record
- Annual review of vehicle use and taxable benefit
- Training policy with objective criteria, such as role or function and development plan
- Prior approval by the supervisor or HR
- Publishing clear selection criteria and subsidy conditions

Assessment

- Standardised evaluation forms and competency models
- Training courses for managers on objective and constructive assessments
- Four-eyes principle, with HR or a more senior manager reviewing evaluations
- Clear agreements on objectives (SMART) at the beginning of the year
- Option for the employee to object or provide feedback in the evaluation report
- Use of scorecards (vendor rating) with automatic reporting
- Documentation of assessment and review points
- Rotation or retesting of regular suppliers after X years
- Competency-based interviewing with standardised questions
- Score forms for each candidate based on predetermined criteria
- At least two assessors per job interview
- Defining objective assessment criteria, such as delivery reliability, quality, price and service
- Restricted access to assessment files (HR/privacy)
- Periodic supplier assessment based on measurable data
- Input from different departments, such as logistics, purchasing and production
- Awareness training on bias and inclusion for recruiters
- Assessment of audit reports by independent persons or a committee
- Mandatory follow-up plan for each audit report, with deadlines and responsible individuals
- Transparent reporting to management or the audit committee
- Risk-based approach to assessing audit findings
- Re-audit or check on improvement measures within six to 12 months
- Use of audit software or tracking tools for follow-up
- Objective selection procedures with test cases or assessments
- Retention of selection reports to substantiate decisions

Enforcement

- Prior approval for high amounts or exceptions
- Checks by the financial administration or accounts on receipts, dates and reasons given
- Analysis of spending patterns to detect misuse
- Reminder of rules of use via intranet or onboarding
- Graduated sanctions framework: warning, then recovery, and finally a fine or HR measure
- Objective and documented determination of the violation
- Maintaining a data register of all processing activities
- Right to be heard before a fine is imposed
- Internal guidelines for proportionate sanctions
- Making an internal escalation procedure or objection procedure available
- Registration of fines imposed and monitoring of repeat offences
- Regular job rotation so that employees do not work in the same role or their own region for too long
- Regular safety audits and workplace inspections
- Up-to-date risk analyses and prevention plans
- Written procedures, toolbox meetings and visible safety instructions
- Training courses and refresher training courses for employees
- Including penalty clauses in contracts with clear conditions
- Privacy by design in systems and processes
- Regular refresher training courses via e-learning or workshops
- Registration of incidents and near misses with follow-up
- Access control for high-risk areas for trained persons only
- Clear code of conduct with examples, including examples of transgressive behaviour

EXAMPLE: MEASURES – CONTINUED

Enforcement – continued

- Training courses on ethical behaviour and integrity
- Mandatory data processing agreements with external processors
- Training courses for employees on privacy-aware conduct
- Clear expenses policy setting out permitted and prohibited expenses
- Access control for personal data (need-to-know)
- Whistleblower Policy
- Publication and signing of the code of conduct upon commencement of employment
- Confidential reporting channel
- Objective sanctions procedure based on the right to be heard
- Clear retention periods and automatic data deletion

Handling information

- Classification of information (public/internal/confidential/secret)
- Policy for handling confidential documents (encryption, destruction, no papers left unattended)
- Training courses on information security and confidentiality
- Restricting access rights based on role or function ('need to know')
- Ban on private storage or sharing via unsecured channels, such as personal email
- Confidentiality agreement upon commencement of employment or cooperation
- Clear processing instructions for each process (collection, storage, use, deletion)
- Always checking consent and the lawfulness of processing in accordance with the GDPR
- Technical measures such as encryption, pseudonymisation and firewalls
- Concluding data processing agreements with external parties
- Data Protection Impact Assessments for high-risk processing operations
- Activating audit trails for sensitive data processing operations
- Logging activities and periodic checks on CRM use
- Restricting the export/download of data
- Regular data cleansing and checks for outdated or incorrect data
- Security policy for devices, such as automatic locking and encrypted hard drives
- Use of Mobile Device Management (MDM) to check settings and apps, and to enable remote wiping
- No private use and no installation of non-approved software/apps
- Mandatory antivirus, VPN and firewall on all devices
- Instructions in the event of loss or theft (immediate reporting, remote blocking)
- Regular checks for updates and patches by IT
- Multi-factor authentication
- Mandatory training in CRM use and data security
- Role-based access control (access only to relevant data)

Handling resources

- Monthly checks on refuelling (location, quantity, type of fuel)
- Mileage tracking or a black box, if permitted
- Duty to report damage, fines and accidents
- Restrictions on fuel cards (no shop purchases, limit per day/week)
- Defined project or departmental budgets with prior approval
- Real-time budget monitoring via dashboards or ERP software
- Mandatory budget check before major expenditure
- Periodic reporting to the relevant managers
- Expenses policy with clear limits, permitted expenses and mandatory supporting documents
- Use of expense claim software with automatic checks (date, duplicates, VAT, limits)
- Logging and monitoring of unusual IT activity, with due regard for privacy rules
- In the event of loss or improper use: duty to report and follow-up by IT or HR
- Cash safe procedure for employees working with cash
- Company car policy with rules on use, maintenance, fines, fuel card and private use
- Proof of receipt of work equipment, for example by signing upon receipt of a car and card
- Alerts in the event of exceeded limits or deviations
- Assignment of one budget holder per department/project
- Approval workflow with segregation of duties
- Mandatory submission within a specified period, for example 30 days
- Spot checks or audit by finance
- Clear communication of the consequences of misuse
- ICT-use policy with guidelines on business use versus limited private use
- Blocking of high-risk websites or apps via network management
- Training courses on cyber-safe behaviour and social engineering
- Mandatory use of VPN, antivirus and screen lock

EXAMPLE: MEASURES – CONTINUED

Third-party contacts

- Declaration by employees of their direct and indirect relationships
- Training courses on competition law (cartel prohibitions, information exchange)
- Rules for networking events and industry meetings
- Prior consent or briefings before taking part in formal meetings
- Ban on sharing competitively sensitive information, such as prices, volumes and strategy
- Option to report inappropriate contact or proposals
- Due diligence on international partners (KYC, sanctions lists, reputation check)
- Use of standard contracts with clauses on anti-corruption, export rules and ethics
- Training courses in export control, anti-corruption and cultural sensitivity
- No cash payments or facilitation payments (bribes)
- Mandatory consultation with the legal or compliance department in the event of doubt or negotiations
- Clear guidelines and scripts for customer communication
- Training courses in recognising social engineering or false proposals
- Training courses in customer-focused, legally correct and empathetic conduct
- Restricting access to customer data to what is necessary
- Monitoring of complaint handling and customer satisfaction
- Escalation procedure for difficult situations or transgressive behaviour
- Authorisation policy: only authorised persons may negotiate or sign
- Presence of two employees during crucial negotiations
- Recording all steps and agreements in writing, in emails or minutes
- Review of contracts by the legal department
- Code of conduct on dealing with suppliers, such as no gifts and transparency
- Checking the origin of contact, such as domain, sender and IP
- Use of an allowlist/blocklist of trusted external contacts
- Mandatory screening of foreign investors or partners
- Not sharing information or entering into contracts without internal consultation
- Screening of employees