MINIMUM CONTROL STANDARDS - 2023

HOLCIM

INTRODUCTION

As a global leader in our industry, **Holcim adheres to the highest of standards** when it comes to how we manage and operate our business day to day everywhere around the world. We see it as our ethical duty.

At the same time, we ensure our license to operate towards government and authorities as well as our employees, investors and the communities where we work.

With this in mind, **first and foremost Holcim complies with all local laws and regulations** where we operate and manage a set of **Minimum Control Standards that every country and business in our organization must follow** – with clear guidance and consequence management.

Minimum Control Standards are the capstone of our Corporate Governance framework and encompass 62 mandatory controls from Governance and Compliance, Fixed Assets, Revenue, HR, Inventory, Expenditure, IT, Accounting and Consolidation, Tax and Treasury to Sustainability.

These minimum control standards are **mandatory throughout our operations**. Each Holcim employee has an important role in ensuring the implementation and effectiveness of our Minimum Control Standards and thus running the Internal Control System.

It is crucial that we engage them in the Minimum Control Standards implementation and ensure that the right organization is in place to improve control effectiveness.

The Minimum Control Standards are **assessed and tested every year** in all our businesses across the globe. Our **local CEOs and CFOs and regional management certify through signed letters** to the Group that they are in place and **operating effectively**.

Group Internal Control

MCS SUMMARY AND CONTENTS

Compliance	Reputational damages	Errors in financials	Operational disruption	Financial losses	Fraud
★	●			●	●
★	●			●	
★	●			●	●
	●				
	●		●	●	
★	●		●	●	
	●		●	●	●
				●	
	●		●	●	
★	●	●	●	●	●
★	●			●	
				●	●
		●		●	●
		●		●	
		●		●	
★	●		●	●	
	●	●	●		
		●			
		●		●	●
★	●			●	●
		●		●	●
★				●	●
		●		●	●
		●		●	●

Compliance	Reputational damages	Errors in financials	Operational disruption	Financial losses	Fraud
★	●	●		●	●
		●		●	
	●			●	
		●		●	
★				●	●
★	●			●	●
		●		●	●
★	●	●		●	●
		●			
		●		●	●
		●		●	●
			●		●
			●		●
			●		●
			●	●	
			●	●	

Compliance	Reputational damages	Errors in financials	Operational disruption	Financial losses	Fraud
		●			●
		●			
		●		●	●
		●		●	
		●		●	●
		●			
		●			
		●			
		●			
		●			
		●		●	
		●		●	
		●		●	
		●		●	
		●		●	
★				●	●
★				●	●
				●	●
		●		●	
				●	
	●		●	●	
★	●		●	●	
	●		●	●	●

Governance and compliance

1 Communication and promotion of the Code of Business Conduct and speak-up culture

PRIMARY OBJECTIVE

Senior management continuously communicate and role model the Code of Business Conduct (CoBC) while promoting a speak-up culture

RISK
- Poor tone at the top (Step 1, 2)
- Corruption and Bribery (Step 1, 2, 3)
- Money Laundering (Step 1, 2, 3)
- Transaction with sanctioned parties (Step 1, 2, 3)
- Infringement of Fair Competition regulations (Step 1, 2, 3)
- Data leakage of sensitive information (incl. non compliance with GDPR) (Step 1, 2, 3)
- Infringement of human rights standards (Step 1, 2, 3)
- Ineffective or unethical vendor selection process (incl. TPDD process) (Step 2)

IMPACT
- Compliance
- Reputational Damages
- Financial Losses
- Fraud

CONTROL & FREQUENCY

1. **CEO communication of the Code of Business Conduct and integrity line to employees at least annually, performance of trainings to risky employees according to the training plan, and acknowledgement of the Code of Business Conduct by newly joined employee, maintained by Human Resources (or designee).** ***Annual***
2. **Communication of the Supplier Code of Conduct to suppliers, outsourced service providers, must be documented.** ***Upon Change***
3. **Remediation by management of any confirmed breach.** ***Upon Request***

REQUIREMENTS

- The Code of Business Conduct (CoBC) is communicated to all new employees, with a short introduction, at on-boarding. New employees acknowledge that they have read and understand the policy and this is stored in the employee's personnel file. The method used for acknowledgment is defined by the local Legal and Human Resource departments (or designated department). (Step 1)
- At least annually and more frequently as the need demands, the CEO communicates to all employees concerning the values of Holcim and the Code of Business Conduct and encourages employees to speak up, report suspected misconduct. (Step 1)
- Employees, with roles and responsibilities that encounter significant Code of Business Conduct risks or have a function of reducing these risks (as defined by local Legal & Compliance) are to undertake periodic training defined locally. (Step 1)
- The integrity line phone number must be working from all our facilities, the access to the website is available through our network and posters should be placed in all our locations, the Integrity Line is communicated in the Intranet, Internet and within or along with the local Supplier Code of Business Conduct. (Step 1)
- The organization's commitment to integrity and ethical behavior as defined in the Supplier Code of Conduct is communicated to the suppliers outsourced service providers (Step 2)
- For existing suppliers, the commitment to our Supplier Code of Conduct is documented through contractual terms and conditions included in the purchase orders and during the tendering process for the new suppliers. In all other contracts, best efforts are made for inclusion of a clause which recognizes the principles of Anti-Bribery and Corruption, as well as Sanctions risk, either referring to our Supplier Code of Business Conduct or our template clause (Step 2)
- In the event that substantiated breaches occur, remediation (consequential management and effect discipline) must occur in consultation with Group Investigations. This process will be governed by the Country General Counsel at country level and Region General Counsel or Head of Compliance above country level. (Step 3)

Link to: Code of Business Conduct, Code of Business Conduct for Suppliers, Anti-Bribery and Corruption Policy, Compliance Policy, Human Rights and Social Policy, Business Integrity and Speaking Up Directive, Sanctions and Export Controls Directive, Human Rights Directive, Third Party Due Diligence Directive, Sustainable Procurement Directive

2 Compliance with Fair Competition laws and requirements

PRIMARY OBJECTIVE

Follow Group Fair Competition Directive, Commercial Documentation Directive and competition law advice and ensure risk-exposed employees are trained

RISK
- Infringement of Fair Competition regulations (Step 1, 2)

IMPACT
- Compliance
- Reputational Damages
- Financial Losses

CONTROL & FREQUENCY

1. **Training on fair competition compliance of highly and medium risk exposed employees is completed and is documented by Local Legal for trainings at country level and Group Legal – Competition Law for trainings at Group Level. *Annual***
2. **Pricing decisions, competitor contacts and sources of market information are documented in accordance with the Commercial Documentation Directive. Advices by Group Legal - Competition Law to Local legal department and business stakeholders are documented. *Upon Request***

REQUIREMENTS

- Employees must comply with the Fair Competition Directive and applicable local competition laws. (Step 1)
- All highly exposed employees must participate in a virtual or physical face to face training every two years; these trainings are organized by the local legal department or if at the Group Level, by Group Legal – Competition Law. All newly recruited highly exposed employees must be trained within 6 months of taking on a job with Holcim. Participation in the virtual or physical face to face training must be documented using a signed participation list or by any other verifiable means (paper or electronic form) with records retained by the Local Legal or if at the Group level, by Group Legal - Competition Law. (Step 1)
- All medium exposed employees must complete an e-learning training every three years; this e-learning training is provided by Group Legal - Competition Law to all Local Legal. All newly recruited medium exposed employees must be trained within six months of taking on a job with Holcim. Successful completion of an e-learning training must be documented by automatic certification generated by the e-learning tool or by any other verifiable means) with records retained by Local Legal or if at the Group level, by Group Legal - Competition Law. (Step 1)
- Employees must comply with the Commercial Documentation Directive to ensure pricing decisions, competitor contacts and sources of market information are properly documented. (Step 2)
- Group Legal – Competition Law regularly advises legal and business stakeholders on competition law compliance by guidance papers or any other means, whenever applicable. (Step 2)

Link to: Compliance Policy, Fair Competition Directive, Commercial Documentation Directive

3 Related party transactions and conflict of interests

PRIMARY OBJECTIVE

Ensure approval of related party transactions by Legal and communication to all employees to declare personal interests that overlap business decisions they need to make

RISK
- Poor tone at the top (Step 2)
- Corruption and Bribery (Step 1, 3, 4, 5)

IMPACT
- Compliance
- Reputational damages
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Monitoring by the appropriate person (see Conflict of Interests directive) and the local compliance officer of potential Conflict of Interests situations reported by employees and any resulting actions or requirements, with documentations kept by local Legal and Compliance department. *Upon Request***
2. **Perform Conflict of Interests communication annually. *Annual***
3. **Review and approval by the legal department before initiating any business deal or arrangement between a Holcim entity and a shareholder or director's company. *Upon Request***
4. **The privileged information on Holcim Ltd, the insiders' list is elaborated and handled at Group level - by Legal & Compliance. Group Legal and Compliance sends the quarterly communication. The insiders' list is cross-checked with HolcimiNK users list. (Group Level) *Quarterly***
5. **The privileged information on a listed Group company, the insiders' list is elaborated and handled at country level - by the Legal department or company secretarial department. The country Legal department sends the quarterly communication. *Quarterly***

3 Related party transactions and conflict of interests

REQUIREMENTS

- Employees are to assess their own situation and disclose any Conflict of Interests (COI) situation to their manager as soon as it becomes apparent. The disclosure will be reviewed as described in the Conflict of Interests directive. (Step 1)
- Training on the Conflict of Interests Directive is a mandatory part of the standard Anti-Bribery and Corruption (ABC) Compliance Training for Employees. (Step 2)
- Conflict of Interests Directive is communicated once a year to enable employees to declare potential conflict of interests. (Step 2)
- Any business deal or arrangement between a Holcim entity and a shareholder or a director's company shall be deemed a related-party transaction. For companies locally listed, related party transactions are to be reviewed by the legal department before approval or signature. (Step 3)
- For Group privileged information, Group Legal and Compliance lists all employees that have access to that information. For other publicly listed entities, the entity legal department may also need to list employees in the entity that have access to privileged information. These lists shall be updated on an ongoing basis. As soon as privileged information such as consolidated financial data and projects data is available internally a communication informing insiders of their obligation not to trade shall be sent out. The updated list and its previous versions as well as the communication is stored by Group Legal & Compliance (or the applicable listed entity). Permissions regarding access to the folder where the lists are stored and secured must be restricted and controlled. (Step 4)
- Group Companies having Securities listed on a stock exchange shall adopt a binding Insider Dealing and Market Disclosure setting at least equivalent standards and processes designed to ensure compliance by that Group Company and its directors and employees of their respective obligations under applicable laws and regulations. Insider Dealing Market Disclosure Directive. (Step 5)

Link to: Compliance Policy, Anti-Bribery and Corruption Policy, Code of Business Conduct, Insider Dealing Market Disclosure Directive, Decisions with Integrity – Conflict of Interest Directive, Conflict of Interest intranet site, Compliance Training Cycle 2022-2024

4 Board of Directors secretarial requirements

PRIMARY OBJECTIVE

The local secretary and the chairperson of the Board of Directors (BoD) ensure that all local corporate legal requirements are met

RISK
- Lack of Board's oversight responsibilities over risk and internal control (Step 1)
- Absence of control and supervision over remote or small entities (Step 1)

IMPACT
- Reputational damages

CONTROL & FREQUENCY

1. Signing by the Board of Directors chairperson and secretary of a letter to confirm compliance with all corporate legal requirements. *Annual*

REQUIREMENTS

When required by law, an entity that has a Board of Directors must ensure that all corporate secretarial duties are performed and documented in a timely manner in accordance with the local requirements. On behalf of the Board of Directors, the secretary and chairperson must ensure that the Board of Directors and its Committees (if applicable) operate according to the provisions of the local corporate laws, company's articles of incorporation, bylaws, charters or other corporate governance regulations. This includes in particular that:

- Key corporate documents and records are maintained in accordance with applicable retention policies (local law and Group regulations)
- Meetings of the Board are held at least as frequently as required by local law
- Minutes are taken at the meetings, are approved and are maintained as part of the corporate records
- Shareholder and Director's registers are kept up-to-date
- Annual shareholders meeting occur, if applicable
- Any other local legal requirements (the defined secretary should specify all the local legal requirements or liase with the local legal team to obtain such information and formalize it.)
- The Board of Directors chairperson and secretary shall jointly confirm compliance with all applicable corporate legal requirements by signing a compliance confirmation letter as part of the annual internal control certification process. Objective of this control is considered achieved with the following alternative measures: 1) in case the CEO is a member of the board, a certification letter signed by the CEO in his/her capacity of a board member and by the secretary; 2) in case the CEO is not a member of the board, a certification letter signed by the CEO and the secretary, presented in the board meeting with formalized meeting minutes signed off by the chairperson of the board.

Link to: Group Delegated Authorities (GDA)

5 Health, Safety & Environment

PRIMARY OBJECTIVE

Ensure effective implementation of the four sections of the Health, Safety & Environment Management System (Leadership and Engagement, Objectives, Planning and Management Review, Operations and Support Processes, Performance Evaluation)

RISK
- Health & Safety issue (injuries, fatalities, illness) or incident (Step 1)

IMPACT
- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

1. **Ensure annually the Health, Safety & Environment policy is correctly applied by verifying the implementation of rewards & recognition and consequence management, Health, Safety & Environment Improvement Plan completion, employees and contractors training plan, Critical Controls and Health, Safety & Environment Key Performance Indicators. *Annual***

REQUIREMENTS

Country must ensure that the following 4 sections of the Health, Safety and Environment management system are in place and operating with regular reviews:

- Leadership and Engagement: Rewards, Recognition and Consequence Management program is in place
- Objectives Planning and Management Review: An annual Health, Safety & Environment Improvement Plan (HSEIP) is set up following the Group process. The Health, Safety & Environment Improvement Plan completion is tracked at the country Executive Committee level and the strategic area of Health, Safety & Environment Improvement Plan is tracked in the Group tracking tool.
- Operations and Support Processes: Ensure that all employees and contractors are in scope of the training plan which must meet minimum expectations of classroom and practical per Health, Safety & Environment standards. Countries must implement the Critical Controls Management as defined by the Group.
- Performance Evaluation: Group Health, Safety & Environment Audit and annual self-assessment performed at unit level. Process Safety Management and Incident Reporting and Investigation with incidents correctly classified and action plans kept up-to-date with relevant actions. Road Key Performance Indicators (KPIs) should be reviewed.

Link to: Health & Safety Policy, Health, Safety and Environment management system, Critical Controls Management, Group Health, Safety & Environment site, Sustainable Procurement Directive

6 Risk assessment

PRIMARY OBJECTIVE

Perform and document a robust business and compliance risk assessment at the country / service center level at minimum annually

RISK
- Poor tone at the top (Step 1, 2)
- Misalignment of the organization with business needs and objectives (Step 1, 2)

IMPACT
- Compliance
- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

1. **A risk assessment is performed annually and documented per Group Risk management process. Action Plans are defined and monitored for all high risks (as a minimum) in accordance with the Risk management guidelines. *Annual***
2. **Country and Service Center risk assessment reports are signed-off by the Country CEOs and the Heads of Service Centers for their respective entities (electronically or physically) and submitted to Group Risk Management. *Annual***

REQUIREMENTS

- A risk lead is appointed in each country to support the local management with the risk assessment process and to monitor mitigation actions. (Step 1)
- A risk assessment is performed and signed off at least annually and identifies risks with the greatest likelihood of occurring and with the highest potential impact as per the current Group Risk assessment methodology (please refer to Group Risk Management guidelines. Risks, risk comments (i.e. description), likelihood (initial and residual), impact (initial and residual) and risk treatment have to be documented in the current Group Risk assessment tool . (Step 1,2)
- Action plans must be defined for all high residual risks (at a minimum) in accordance with the Group Risk Management guidelines. Action plans (title and description), owner and due date have to be documented in the risk management tool. (Step 1)
- Update of the status of actions in the risk management tool is done when the risk assessment is performed as per the Group requirement.(Step 1)

Link to: Finance Policy

7 Mitigation of business risks - Security

PRIMARY OBJECTIVE

Implement security measures and procedures in accordance with the Security & Resilience Policy.

RISK
- Assault on person (Step 1, 2)
- Attack against business asset (Step 1, 2)
- Theft (Step 1, 2)

IMPACT
- Reputational damages
- Operational disruption
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Annual sign off by the Country Chief Executive Officer (CCEO) of the Country Ecosystem report and Country Security Risk Assessment.** ***Annual***
2. **Ensure minimum implementation requirements of the Security and Resilience policy, the Security & Resilience Management System (SRMS), and directives are completed by the Country Security Representative.** ***Annual***

REQUIREMENTS

Country must implement and manage a Security and Resilience programme, based on the Security and Resilience Policy, the Security & Resilience Management System (SRMS) and the Security Directives. This requirement includes functions or other horizontal teams who may operate within existing Holcim countries but have unique risk profile (Holcim Trading, Holcim Energy Solutions, IT Services Centers, Business Services Centers, etc). In case of joint Security programme with a Holcim Country, a formal agreement should exist.

At a minimum, the Country must perform the following tasks:

- Ecosystem: capture on an annual basis the country ecosystem (people, assets, etc) in the Holcim Sites mapping application, including evacuation People on Board (POB), where applicable. (Step 1)
- Risks: conduct security and resilience risk assessment at country level on annual basis (Step 1)
- Minimum implementation requirements (Step 2)

a. Structure: CEO must appoint a fit for purpose Country Security Representative (CSR) and relevant organization to successfully implement the programme. Mandatory trainings are completed and documented for the relevant stakeholders.

b. Budget : Report total FY-1 spend, publish dedicated security budget for FY-0 and validate security related spend on a quarterly basis in the Sites Mapping Application.

c. Mitigation controls: implement mitigation controls at the location of the risk and deploy specific programmes where Group Level Material Risks (GLMRs) and Directives (SSI, TOC) have been identified as "in-scope".

d. Travel: A Country Travel & Event Policy is in place, as per the Group Travel and Events Policy. Appoint a Country Travel Coordinator; travel agency(ies) are connected to I-SOS Travel Tracker; the Travel dashboard weekly extract is systematically used to verify visibility of all international business travelers in the Travel Tracker and that they've completed the general business travel eLearning. The Country Travel Guide is updated annually.

e. Third Parties: Engage, Manage and Evaluate suppliers providing security services in line with Holcim processes.

f. Incident response: report all security incidents through Holcim Security Incident Notification Tool (SINT) and provide evidence that all High & Very High (attempted) incidents have documented lessons learned and related action plans.

- Assessment, Assurance and Performance: (Step 2)

a. Track the implementation of the Security & Resilience Management System and the deployment of directives;

b. Send the Country Security & Resilience Briefing to Country Chief Executive Officer (CCEO) and Group Security & Resilience at least annually

Link to: Security and Resilience Policy, People Security Directive, Security Services with Integrity (SSI) Directive, Terrorist & Organised Crime (TOC) Monitoring Programme Directive, Travel and Events Policy, Security & Resilience Management System (SRMS)

The above requirements can be performed more frequently in response to a significant change to the business or risk landscape, or if specifically mandated by Group Security and Resilience Governance requirements

8 Mitigation of business risks - Group insurance

PRIMARY OBJECTIVE

Follow the Group insurance process to ensure adequate risk coverage

RISK
- Lack of insurance coverage (Step 1, 2, 3, 4, 5)

IMPACT
- Financial losses

CONTROL & FREQUENCY

1. **Payment of Group insurance premiums is done prior to the due date.** ***Annual***
2. **Annual approval by the local Executive Committee (or designee) of property insurance values for accuracy according to Group methodology, to ensure replacement value cover.** ***Annual***
3. **By using Group Risk Insurance Tool Incident Report is submitted within 48 hours by the local Executive Committee (or designee) for all claims and losses that are covered by a Group Insurance policy and that are likely to exceed the applicable deductible or exceed EUR 500'000 (or equivalent).** ***Upon Request***
4. **Group Insurance and Risk Financing is informed: 1) before new business activity is put in place, 2) of all Capex projects in excess of EUR 5m, 3) of any Risk Improvement Actions (RIA) countries do not agree with.** ***Upon Change***
5. **Local Executive Committee approves purchase of additional local insurances for risks that are not covered by a Group insurance program.** ***Upon Request***

REQUIREMENTS

The Country must comply with the following 5 priorities:

- Group insurance premiums are paid by the due date with no delay. (Step 1)
- Property insurance values are provided annually to Group Insurance and Risk Financing (GIRF) before the due date to avoid under-insurance. (Step 2)
- All claims and losses that are covered by a Group Insurance policy and that are likely to exceed the applicable deductible or exceed EUR 500'000 (or equivalent) have been timely declared to Group Insurance and Risk Financing (GIRF) within 48 hours of incident via Group Risk Insurance Tool (GRIT) . (Step 3)
- All Risk Improvement Actions (RIA) recommended by our insurer have to be mitigated within a reasonable time frame. If Group Countries do not agree with the RIA, GIRF must be notified and alternative measures must be put in place. (Step 4)
- Any change in the business that impacts the Group Insurance programs* are communicated to Group Insurance and Risk Financing (GIRF) (e.g. new business activity like installation of building materials, new products with different liability risks such as building material chemicals, etc.). (Step 4)
- All Capex projects in excess of EUR 5m (or equivalent) are reported to Group Insurance and Risk Financing (GIRF) to ensure appropriate coverage. (Step 4)
- For risks that are not covered by Group insurance programs*: (Step 5)
  a. Local Executive Committee must put in place local insurances as required by local regulations (e.g. motor liability, workers compensation insurance)
  b. Local Executive Committee may put in place local insurance for non-mandatory local risks as long as these do not overlap Group insurance programs (e.g. allowed would be fiduciary insurance for local pension fund, trade credit insurance)

Link to: Finance Policy, Group Insurance Directive, Capex Directive, Group insurance program

Group insurance programs:

- *Property Damage / Business Interruption (PDBI); Third Party Liability (TPL); Directors & Officers (D&O); Marine Protection & Indemnity and Charterers Liability; Marine Cargo and Cyber*
- *Construction All Risk / Erection All Risk (CAR/ EAR) – alternative local insurance allowed if cleared by Group Insurance and Risk Financing before project commences*

Group Insurance and Risk Financing is regularly reviewing the risks situation and reserves the right to define other risks to be covered by a Group insurance program

9 Mitigation of business risks - Business Resilience System

PRIMARY OBJECTIVE

Every country must have a Business Resilience System

RISK
- Assault on person (Step 1)
- Supply chain disruption (Step 1)
- Business disruption due to IT/OT unavailability (Step 1)
- Attack against business asset (Step 1)

IMPACT
- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

1. **Annually verify that the following requirements are in place in accordance with the Holcim Business Resilience Directive - *Annual*:**
   - **a. Appointed Business Resilience Sponsor, Business Resilience Coordinator and Business Resilience Team**
   - **b. Current Country Business Resilience Plan ('Plan on a Page').**
   - **c. Crisis Management Plan and Business Continuity Plan at country level, Emergency Response Plan available at the location of the risk(s).**
   - **d. Specific country level plans for Group Level Material Risks, High and Very High initial risks identified.**
   - **e. Post-exercise report which includes objectives, the risk being exercised and the lessons learnt.**

REQUIREMENTS

All Holcim countries must implement and manage a Business Resilience (BR) programme, following their Security and Resilience Management System (SRMS) and the Business Resilience directive requirements. The Country CEO (CCEO) must determine, based on the risk, whether a Business Resilience programme is required in addition at the sub-country level. This requirement includes functions or other horizontal teams who may operate within existing Holcim countries but have unique risk profile (Holcim Trading, Holcim Energy Solutions, IT Services Centers, Business Services Centers, etc). In case of joint Business Resilience programme with a Holcim Country, a formal agreement should exist.

Each country must:

- Nominate a Business Resilience Sponsor and a Coordinator to implement the Business Resilience programme. Appoint a Business Resilience Team (BRT) consisting at a minimum of Business Resilience Team leader and core members
- Perform and document annually the training of Business Resilience sponsor, Coordinator and Business Resilience Team
- Prepare a Country Business Resilience Plan ('Plan on a Page') as per the Business Resilience Directive
- Maintain specific country level plans for Group Level Material Risks (GLMRs), High and Very High initial risks identified in the Holcim Security and Resilience Risk assessment tool
- Perform an annual Business Resilience Team exercise based on your risk assessment

Link to: Security and Resilience Policy, Business Resilience directive

10 Mitigation of business risks - Remediation of deficiencies and non-compliance with MCS

PRIMARY OBJECTIVE

Management process is in place to identify and correct deficiencies found while monitoring the MCS

RISK
- Poor tone at the top (Step 1)
- Misalignment of the organization with business needs and objectives (Step 1, 2)

IMPACT
- Compliance
- Reputational damages
- Errors in financials
- Operational disruption
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Approval by Group Head of Function and Group Internal Control for local control design which do not agree/ comply with Minimum Control Standards requirements/central description. Validation by Regional IC correspondent of Not Applicable controls. Deficiencies to Minimum Control Standards are approved by Region Head (for Countries) /Group management (for Functions) through the certification process. *Annual***
2. **Monitoring by the local Executive Committee of the progress of all action plans relating to deficiencies to ensure they are resolved and reported to the Group according to Internal Control instructions. *Half year***

10 Mitigation of business risks - Remediation of deficiencies and non-compliance with MCS

REQUIREMENTS

Management responds timely and appropriately to any deficiencies identified through monitoring activities of and takes adequate and timely actions to correct deficiencies. This process includes:

- The MCS exception approval process: In case a country is not able to design a local control description in compliance with the Minimum Control Standards (MCS) requirements, ("Requirements" + "Control Description"), the Country internal control manager clears with Regional IC correspondent, uses the MCS Design and Implementation non-compliance approval form to seek Group approval. Submission must be done two weeks prior to the Control Design Assessment (CDA) deadlines. Approvals are to be uploaded/linked at SAP Governance, Risk, and Compliance tool (SAP-GRC). (Step 1)
- Controls rated as Not Applicable and split of responsibility among entities and Service Centers must be formally validated by Regional Internal Control correspondent. (Step 1)
- Deficiencies to Minimum Control Standards has to be validated by local management, Region Head (for Countries) /Group management (for Functions) through the certification process. (Step 1)
- Any deficiency related to MCS classified with an impact over Compliance: MCS# 01, 02, 03, 06, 10, 11, 16, 20, 22, 25, 29, 30, 32, 56, 57, 62. (MCS01.01/02/03; MCS02.01/02; MCS03.01/02/03/04/05; MCS06.01/02, MCS10.01/02; MCS11.01/02; MCS16.01/02/03/04; MCS20.01/02; MCS22.02, MCS25.01; MCS29.01; MCS30.01/02; MCS32.01/02; MCS56.02; MCS57.01, MCS62.05) must be approved by the Regional Compliance Officer before signature of the Country Certification Package. (Step 1)
- Perform root cause analysis, a detailed description of the deficiency and the creation of an action plan to remediate the weakness identified. (Step 2)
- Deficiencies are communicated to those parties responsible for taking corrective action, at senior management (Step 2)
- Follow-up of corrective actions and progress towards completion. (Step 2)
- Action plans relating to deficiencies are tracked regularly by the local Executive Committee and to Group Internal Control at least twice a year. (Step 2)
- All deficiencies and action plans are tracked in SAP Governance, Risk, and Compliance tool (SAP-GRC). (Step 2)

Link to: Finance Policy, MCS Design and Implementation non-compliance approval form , Internal Control Instructions, Holcim Financial , Certification Permanent Instructions

11 Personal data protection

PRIMARY OBJECTIVE

Ensure personal data/ personally identifiable information (PII) managed in the company (acquired, processed, stored and deleted) is handled in accordance with local laws and regulations

RISK

- Unauthorized use of company & personal information (incl. non compliance with GDPR) (Step 1, 2)
- Data leakage of sensitive information (incl. non compliance with GDPR) (Step 1, 2)

IMPACT

- Compliance
- Reputational damages
- Financial losses

CONTROL & FREQUENCY

1. **Train employees in scope, as per the country defined training cycle, on how to comply with local Data Protection laws and regulations as well as on recognizing and reporting data breaches. *Annual***
2. **Implement Data Subject Consent Form (in local language, if necessary) for different types of data subjects (e.g. candidates, employees, customers, suppliers) if required by local data protection law. Annual verification with each department that Data Processing Agreements are signed with vendors processing Personal Data on Holcim behalf. *Annual***

11 Personal data protection

REQUIREMENTS

If required by the local data protection and privacy laws and regulations,

- The Data Privacy Notice/Policy is made available to all existing employees and distributed to new employees during the onboarding process. (Step 1)
- If required by the local data protection and privacy laws and regulations, relevant employees are trained to recognize and report data breaches or any incidents relating to personal data which may carry reporting/notification obligations. Country is free to determine who are relevant employees.(Step 1)
- Countries are required to define a compliance training program for a locally defined cycle. They define what training they want to deliver, and which is the target population within what time period. All newly recruited relevant employees must be trained within 6 months of taking on a job with Holcim. (Step 1)
- Seek advice from the Data Protection Responsible / Legal and Compliance if necessary. (Link to the control standard on employee onboarding). (Step 1, 2)
- Consent is collected and recorded when the employee's image (photo/video) is taken and used by the company.(Step 2)
- Data Privacy Notice/Policy is made available / distributed to all existing, new customers and prospects (either by email, online on a dedicated customer platform or on the company's website, addendum to the existing commercial contract, or it is embedded into the general terms and conditions of the commercial agreement). (Step 2)
- Customer's consent is collected and recorded whenever required. Seek advice from the Data Protection Responsible / Legal and Compliance concerning the collection of customer consents. (Link to the control standard on customer master data).(Step 2)
- If required by the local data protection and privacy laws and regulations, when external vendors have access to personal data/PII handled by a Holcim entity, seek advice from the Data Protection Responsible / Legal and Compliance concerning implementation of an agreement with the vendors regarding the processing and protection of that personal data/ PII. (Step 2)
- If required by the local data protection and privacy laws and regulations, a process is put in place and communicated internally to respond to data subject requests concerning an individual's personal data processed by the company. Always inform and seek advice from the Data Protection Responsible/ Legal and Compliance concerning how to respond to a data subject request. (Step 2)

Link to: Compliance Policy, General Data Protection Directive, Data Retention and Deletion Directive

12 Segregation of duties and user access review

PRIMARY OBJECTIVE

Ensure there is a proper segregation of duties and users have need based access to IT applications.

RISK
- Unauthorized access, disclosure, modification, damage or loss of data (Step 1, 2, 3, 4)

IMPACT
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Information Technology Service Centers annually review and validates the Segregation of Duties rule set for Enterprise Resource Planning (ERP) system, other in-scope applications per region and provides the confirmation to the Countries / Functions / Service Centers. *Annual***
2. **Review half yearly, at a minimum, of the Enterprise Resource Planning (ERP) system, other in-scope applications per region Segregation of Duties reports by the respective Business Process Owners and the CFO. Segregation of Duties conflicts are removed or mitigated as per the Group requirements. *Half year***
3. **Validation half yearly, at a minimum, over users' level of access for all critical business applications including TIS and corrective actions taken within one month after the review, if needed. *Half year***
4. **Validation half yearly, at a minimum, over dormant users access deletion/ revoked, and corrective actions taken within one month after the review, if needed. *Half year***

12 Segregation of duties and user access review

REQUIREMENTS

Segregation of Duties (SoD):

- Information Technology Service Centers (ITSCs) annually review the Segregation of Duties (SoD) rule set for Enterprise Resource Planning (ERP) system and other regionally scoped applications for SoD, to ensure alignment with Group rules and update the local customized objects (transactions) with support from business and provides the confirmation to the Countries / Functions / Service Centers. Where the Segregation of Duties (SoD) ruleset is managed directly by the Countries, this should be performed at Country. (Step 1)
- Risk with zero conflicts (RWZC) are eliminated upon identification. There is no tolerance for conflicts over risks mapped as "Risk with zero conflicts". (Step 2)
- Other SoD risks (non RWZC) are to be kept at a minimum. Whenever removal is not possible, they are mitigated by implementing a compensating control. These compensating actions must be documented and monitored to ensure they are reducing the identified risk. The compensating controls must be tested for operating effectiveness. (Step 2)
- Exceptions of the above, Risk with zero conflicts and non-Risk with zero conflicts requirements, have to be reviewed and agreed with Internal Control Regional Correspondent and approved by the Head of Group Internal Control (Step 2)

Business Access Review:

At least twice a year, the following occurs for all critical business application including TIS*:

- A review of all user accounts to ensure that users have access according to their job roles. Any excessive access that is not required for the performance of their job role should be revoked within one month from the date of identification. (Step 3)
- IT should provide a report for all business users with the level of access for business to review user access rights to ensure that the access is in line with their job role. Business must propose corrective actions (e.g. revoke access / change access and send a request to IT for such changes) to be supported by the IT team (Step 3) .
- Business must obtain the dormant user report from IT for all critical business applications and review to ensure that dormant users access is timely revoked / deleted (notify IT to disable/ delete dormant user ID's). (Step 4)

Link to: Finance Policy, Annex 10 Holcim SoD conflicts (RWZC), Annex 10.02 Holcim SAP SoD ruleset, Annex 09 IT Controls, Annex 09.02 TIS roles and security management

**Critical business applications are defined and documented as per Annex 09 IT Controls*

13 Delegation of authorities and approval workflows

PRIMARY OBJECTIVE

Define clear delegation of authority in compliance with Group Delegated Authorities with an adequate approval system

RISK
- Authority and responsibility not clearly and formally assigned (Step 1)
- Unauthorised transactions/ contracts made on the behalf of Holcim (Step 2, 3, 4)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Approval by the local Executive Committee (and Board of Directors, if applicable) of the authorization policy which includes Group Delegated Authorities requirements.** ***Annual***
2. **Any contractual commitment included in the Group Delegated Authorities entered into by the company must bear dual signature of the authorized persons defined in the local delegation of authority matrix.** ***Upon Request***
3. **Review and approval by the manager responsible for the workflow approval matrix (system or manual) for compliance with the authorization policy. For any manual approval processes the method of documentation are to be defined and evidence must be maintained for each approval.** ***Half year***
4. **Half yearly verification by the manager responsible of users set up in the approval workflows in the Enterprise Resource Planning (ERP) system (e.g. the users mapped to release groups). Exceptions, if any, should be investigated. Review of users with authorization to update the release groups is performed, errors analyzed and corrected.** ***Half year***

13 Delegation of authorities and approval workflows

REQUIREMENTS

Group Delegated Authorities (GDA): The Group defines approving authority and threshold for key transactions and commitments involving Holcim or any of its subsidiaries. These rules provide a framework to the countries and functions to make their decisions. These rules must be complied with and all approvals must be documented. (Step 1, 2)

Defining the local Delegation of Authority Matrix: (Step 1, 2)

- An authorization policy or delegation of authority (DoA) matrix must exist to establish clear lines of authority for the approval of all main transactions within monetary limits and other authorizations in the Country, such as the signing authorities. As monetary thresholds increase, additional approvals from senior levels of management are required, with the highest monetary thresholds requiring Board of Directors and Executive Committee's approval. This delegation of authority is formally documented, kept up-to-date and signed-off by the local Executive Committee, and Board of Directors (when applicable).
- Group Delegated Authorities must be respected within the country delegation of authority matrix. Country authorities and threshold defined in the Group Delegated Authorities may be delegated locally but such must be documented in the local delegation of authority (DoA) and approved by the local Executive Committee (and Board of Directors, if applicable).
- Responsibilities are clearly stated and communicated within the organization.
- The assignment of responsibilities is clear, including third-party service providers (who carry out activities on behalf of the organization), related to the extent of their decision-making rights.
- The delegation of authority is adhered to for every transaction which requires approval.
- The delegation of authority matrix is reviewed at least yearly for compliance with the authorization policy or limits definitions and updated as needed.

Maintaining the Delegation of Authority Matrix in the system: (Step 3, 4)

- The delegation of authority is loaded in the Enterprise Resource Planning (ERP) system workflow approval matrix. This and any subsequent changes require appropriate approval based on supporting documentation.
- Half yearly, a report is run of all users set up in the release groups (authorized approvers) to verify that they are in line with the local approved delegation of authority, which respects the Group Delegated Authorities. The report is reviewed and signed-off by the manager responsible. Access to update the release groups is restricted to authorized users.

Link to: Group Delegated Authorities (GDA), Finance Policy

14 Litigation disputes

PRIMARY OBJECTIVE

Risks related to legal disputes are assessed and recorded quarterly in the Group Legal Case Management tool

RISK

- Failure in litigation management (Step 1, 2)
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2)

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Quarterly approval by the country Head of Legal (or designee) of the information reported in the Case Management tool to Group Legal to ensure all required information is reported, complete and updated with the latest assumptions according to Group Legal requirements.** ***Quarterly***
2. **Quarterly review by the local CFO (or designee) of the provisions reported in the Case Management Tool to confirm they correspond with the amounts in the financial statements.** ***Quarterly***

REQUIREMENTS

- The legal department keeps track of and properly completes the status of all ongoing disputes, including the estimated maximum risk, estimated expected risk, classification of the risk as probable, possible or remote and the related provisions recorded in the financial statements. (Step 1)
- At year-end (minimum), legal opinion letters shall be requested from external law firms assisting on disputes to receive updated information regarding such disputes. The legal opinions are reviewed by the legal department and CFO. (Step 1)
- The Group Legal Case Management tool must be updated as per the Group Legal reporting requirements. At a minimum provision amounts and the classification of the risk in the Case Management tool must correspond with to the amounts recorded in the financial statements at that date. The estimated maximum risk, the classification of the risk and the provisions are reviewed by the CFO. (Step 2)
- Control must be performed at least every quarter at closing, and it's a requirement for the execution of the Financial Certifications. (Step 2)

Link to: Group Delegated Authorities (GDA), Data Retention and Deletion Directive, Group Legal Case Management tool

15 Review of contracts by finance

PRIMARY OBJECTIVE

Contracts and material commitments are reviewed by Finance

RISK
- Unauthorised transactions/ contracts made on behalf of Holcim (Step 1, 2)
- Lack of contract management (Step 1)
- Non-adherence to accounting and reporting requirements and standards (Step 1, 2)
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 2)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Review and approval by CFO (or designee) of contracts in a foreign currency, leases and all material commitments to ensure proper accounting, foreign exchange risk management and disclosure before signing or upon subsequent change.** ***Upon Request***
2. **Approval by the CFO of the accounting impact of significant leases based on locally defined thresholds and Group Lease Directive (including material, complex and judgmental contracts).** ***Upon Request***

REQUIREMENTS

- Each entity should determine the scope or defined criteria of contracts to be reviewed by finance based on country's materiality as per SAP- Financial Consolidation (SAP-FC) report P780-050. For Leases apply the Group Lease Directive. (Step 1,2)
- Contracts are reviewed by finance prior to signing to ensure: (Step 1,2)
  - Contracts in a foreign currency are communicated to the local financial department and approved by CFO (or designee) before signature.
  - Financial impacts are properly assessed, and are taken into account in the decision making (capital expenditures (CAPEX), operating expenses (OPEX), leases per International Financial Reporting Standards 16 (IFRS 16), take or pay, off balance sheet clauses, power purchase agreements (PPA), etc.).
  - All material commitments are communicated to the financial department to ensure proper accounting and disclosure notably for the Group external publication.
  - For International Financial Reporting Standards 16 (IFRS 16) before signing the agreement, leases must be formally approved according to the threshold and the approvers defined in the Lease Directive to ensure correctness of the data captured from each contract (or change to a contract), as well as the determination and valuation of the additional valuation parameters (interest rates, probable end date, etc). Countries are asked to avoid any leases that result in a foreign exchange exposure (FOREX). Therefore, all leases that are not denominated in the functional currency of the country always require a separate approval from Group Treasury (regardless of whether leases are budgeted or not).
  - In addition all contracts related to the control assessment or scope of consolidation such as acquisition or divestment contract, put or call option contracts, shareholders agreement, must be reviewed and communicated to Group Finance (HARP 4.1.5.3).
- During the Request for Proposal (RfP) process, a financial review must occur to support the business decision to buy or lease an asset, including assessment of the financing method (by treasury) and the potential impacts to the financial statements (from accounting expert). See Lease Directive sections 2.1 and 2.2. (Step 1,2)
- In the case of a volume increase or scope changes during the life of a contract involving foreign currency, all changes must be communicated to finance for further actions. (Step 1,2)

Link to: Group Delegated Authorities (GDA), Finance Policy, Procurement Policy, Lease Directive, CAPEX Directive, Foreign Exchange (FX) & Interest Rate (IR) Risk Management Directive, HARP 4.2.1 and IFRS 16 checklist & simulation model, 4.1.5.3 Accounting for Put and Call Options on Non-Controlling Interests

Fixed assets

16 Management of titles, licenses and permits

PRIMARY OBJECTIVE

Ensure proper validity, filing and timely renewal of titles, licenses and permits.

RISK
- Lack of valid titles, licenses and permits (Step 1, 2, 3, 4)
- Unauthorized land and quarry usage (Step 1, 2, 3, 4)
- Corruption and bribery (Step 1, 2, 3, 4)

IMPACT
- Compliance
- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

1. **Annual approval by local CEO of the list of all relevant permits & licenses for the business to operate. *Annual***
2. **Annual approval by the local legal team (or equivalent at your organization) and the quarry (mine planer) and land management officer (or equivalent at your organization) of the existing titles of ownership, mining and surface rights, concessions and permits, including upcoming renewals. *Annual***
3. **Approval, half yearly, by the land management officer (or equivalent at your organization) of the land ownership situation, including proposed or planned land activity (acquisition, disposal), and the effect on the relevant licenses. *Half year***
4. **Annual approval by stakeholders (see requirements) of the progress of mining activities and the compliance with mining regulations and permit requirements. *Annual***

REQUIREMENTS

- For all relevant permits & licenses (e.g. environmental, operating permits, quarry & mining, production, energy use, vessels & ports, construction, air, water, deforestation, blasting), roles and responsibilities are clearly defined within the organization, adequate processes are put in place in order to ensure their validity , proper filing & archiving, timely renewal, and publication (if required). The list is updated and clear ownership is assigned together with a procedure for management of different types of permit and licenses (Step 1)
- Local laws and regulations, international standards when required, as well as Holcim Code of Business Conduct (CoBC), are respected in the management of all permits & licenses related activities. (Step 1)
- Third Party interfacing with public officials to acquire, renew or review titles, licenses and permits are managed through the Third Party Due Diligence (TPDD) tool. (control related to TPDD is covered in MCS30) (Step 1)
- All existing titles of ownership, mining / surface rights, concessions and permits are reviewed at least annually with the local legal team (or equivalent at your organization) and in consultation with the quarry (mine planner) and land management officer to ensure they are valid. (Step 2)
- The land management officer leads a review of the land ownership situation twice a year (or according to the local requirements). A review of the foreseen land acquisition / disposals is led by the land management officer with the quarry management and the country raw material competent person. These reviews covers all requirements to maintain the relevant licenses and permits. (Step 3)
- Renewal of permits, trigger and exercise of mining rights and permits occurs before the expiration date. (Step 3)
- Meetings with all stakeholders are conducted to review the progress of the mining activities, monitor compliance with the mining regulations and permitting obligations. These include Quarry & Plant Management, Sustainable Development, Environment, Legal and Land Management. (Step 4)

Link to: Code of Business Conduct, Third Party Due Diligence Directive, Technical Recommendation: Land Management, Holcim Raw Material Resources and Reserves Reporting Standard

17 Quarry reserves and provisions for restoration and rehabilitation

PRIMARY OBJECTIVE

Ensure that quarry reserves are secured, restoration and rehabilitation requirements are implemented for every quarry and properly recorded in financial statements

RISK

- Failure in quarry rehabilitation and biodiversity management (Step 1, 3, 4)
- Depletion of our own reserves (Step 1, 4)
- Non-adherence to accounting and reporting requirements and standards (Step 2)
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 4)

IMPACT

- Reputational damages
- Operational disruption
- Errors in financials

CONTROL & FREQUENCY

1. **Annual reconciliation of the resources and reserves with the total of extracted tonnages transmitted to the accounting department based on the yearly estimates and approval by CFO. Cases where the remaining useful lives of plants and equipments are greater than the remaining secured reserves must be reported in the financial certification package.** ***Annual***
2. **Annual verification by finance and land and quarry management of the validity of the restoration / rehabilitation concept and costs as well as the assumptions used to calculate the provisions.** ***Annual***
3. **Verify if the quarry is classified as high biodiversity importance according to criteria for biodiversity importance category (BIC 1 and 2). If yes, annual review of Biodiversity Management Plan (BMP) by an expert to ensure that actions being implemented properly address the site biodiversity issues. Biodiversity roadmaps integrated in CEM Plant Development Plans (PDP).** ***Annual***
4. **Review and validation by legal of contracts relating to the rehabilitation / restoration work prior to signing.** ***Upon Request***

REQUIREMENTS

- Reserves for cement production sites must be classified according the Raw Material Resources and Reserves Reporting Standard. On a yearly basis, Raw Material Resources and Reserves as well as raw mix lifetime figures have to be reviewed and validated by a Holcim Competent Person and reported according to the business cycle requirements defined by the Plant Development Plan (PDP) as per the Raw Material Resources and Reserves Reporting Standard. Aggregates resource and reserves are classified according to HARP definitions. Each Country shall report yearly raw material Resources & Reserves according to the business cycle requirements defined by Aggregates Reserves Management (ARM). (Step 1)The yearly estimate of the reserves are reconciled with the total of extracted tonnages transmitted to the accounting department. (Step 1)
- All resources and reserves acquired are correctly reflected in the accounts and do not lead to any impairment issues. Cases where the useful lives of the plants and equipment are greater than the remaining secured reserves for cement and aggregates sites, the related action plans must be developed and reported in the financial certification package. (Step 1)
- A restoration/rehabilitation plan for each quarry operation must be developed according to Group requirements and in line with the intended long-term development of the quarry site, specifying the magnitude and schedule of restoration/ rehabilitation work. The plan and its supporting documents are available from both land & quarry management and finance. (Step 2)
- The cost of restoration/rehabilitation work, based on local historical data or estimates given by recognized specialists, is verified and approved by the Country plant management and is included as an annex to the plan, allowing the assumptions to be verified. (Step 2)
- At least once a year, finance and land and quarry management, with legal if necessary, meets to review the validity of the restoration/rehabilitation concept as well as the evaluation of related costs and validate assumptions used to calculate site restoration/ rehabilitation provisions (discount rate, timing of future cash costs, residual life, etc.). If a revision occurs that impacts a legal guarantee related to rehabilitation, finance will secure the corresponding revision. (Step 2)
- A Biodiversity Management Plan (BMP) must be in place for quarries categorized as of high biodiversity importance according to the criteria for biodiversity importance category (BIC. 1 and 2) (Step 3)
- Biodiversity Index (BIRS) baseline roadmap must be established in all managed land (active, inactive and closed sites). For cement sites, it must be integrated in the CEM Plant Development Plans (PDP) (Step 3).
- Materials used for restoration must be compliant to the Health, Safety and Environment (HSE) Internally Generated Waste standard (Step 4)
- Restoration/rehabilitation work contracts must be reviewed on regulatory aspects by Legal expert prior to signing and are copied to finance for filing. (Step 4)

Link to: Finance Policy, Raw Material Resources and Reserves Reporting Standard, Aggregates Reserves Management (ARM), Criteria for biodiversity importance category (BIC. 1 and 2),Quarry Rehabilitation and Biodiversity Directive, Health, Safety and Environment (HSE) Internally Generated Waste standard, Lease Directive, Capex Directive

HARP references: 4.10.2 Site Restoration Costs, 6.6.5.3 Raw Material Reserves / 6.6.5.2 Raw Material Resources

- *The life (but only for AGG) is defined by 60.6.5.05 Reserves Life [yrs]*
- *Accounting is specified in: 4.10.3 Amortization of Raw Material Reserves and 4.10.2 Site restoration*
- *Capex classification defines how to report the purchase: 3.1.8.2 Classification of CAPEX*
- *4.2.1 Accounting for Leases under IFRS 16 - defines specific exemptions related to reserves, when we rent the land*
- *3.2.1.2.28 Depreciation and Amortization of Long-Term Operating Assets - defines depreciation of raw material reserves and capitalized mining concessions*

18 Classification and depreciation of fixed assets

PRIMARY OBJECTIVE

Ensure the proper recognition and classification of fixed assets in the financial statements.

RISK
- Inaccurate or fraudulent recording of fixed assets (Step 2, 3)
- Non-adherence to accounting and reporting requirements and standards (Step 1)
- Inaccurate or fraudulent closing entries (incl. judgemental assumptions and estimates) (Step 3)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Approval by the appropriate finance person to capitalize an expenditure according to the HARP classifications and assign the proper life and depreciation methods. *Quarterly***
2. **Quarterly approval by the appropriate finance person of the Construction in Progress accounts to ensure that only active projects are included (i.e. non viable projects are written off and completed projects are moved to Property, Plant and Equipment). *Quarterly***
3. **Approval by the CFO (or designee) of the write-off of all unused, mothballed and idle assets and/or change of depreciation method used. *Upon Request***

REQUIREMENTS

- Assets are properly classified. Refer to HARP 3.1.1.2.4 Property, Plant and equipment, 4.4 Capitalization, Accounting and Valuation of Assets and 4.2 Accounting for Leases. Lease Directive, CAPEX Directive (Step 1)
- Depreciation schedules required for different purposes are maintained. Refer to HARP 3.2.3.5 Ordinary depreciation and amortization and 4.4.4 Useful Lives of Property, Plant and Equipment. (Step 1)
- For mineral reserves, refer to HARP 3.1.1.2.4 (section 3 Land and Mineral Reserves). (Step 1)
- Capitalization of the expenditure and the timely initiation of depreciation are reviewed and approved by the appropriate Finance person. Journal entries, if needed, have attached the supporting calculation and are signed off by the the appropriate Finance person. (Step 1)
- The person responsible for Construction in Progress (CIP) reviews the status of all Construction in Progress to check whether assets, with a value deemed recoverable, are ready for use. Any change related to the project and the use of the asset should be taken into account in the assessment of the irrecoverability of the asset value. Based on this review, finance staff responsible for Property, Plant and Equipment (PPE) reclassifies Construction in Progress to fixed assets and initiates depreciation within 30 days of the recorded actual finish date. Any journal entries made are reviewed to ensure proper classification and approved. HARP 3.1.1.2.4 (Step 2)
- Accelerated depreciation of an asset might be required if a tangible asset becomes obsolete, is replaced earlier than expected, or cannot be used anymore as a result of newly introduced stringent environmental measures. (Step 3)
- Once assets are identified as unused, mothballed or idle, the depreciation and the assumptions should be supported by adequate documentation and properly approved by the CFO (or designee). Unused, mothballed and idle assets that have been written-off are supported by adequate documentation and are approved by the CFO, as well as change of depreciation method (incl. Reduction of useful life). Refer to HARP G 002-13 Mothballing 2013 in section 3.1.1.2.4. (section 2.10 Idle Assets). (Step 3)
- Group Sustainability targets which might trigger additional investment in proven technologies resulting in certain assets being idle or obsolete in a shorter period than the original estimated useful life of the assets. This should be reviewed carefully with the Regional CFO and accelerated depreciation might have to be accounted for. (Step 3)

Link to: Finance Policy, Lease Directive, CAPEX Directive and Annual ARC impairment model and impairment testing guidelines.

19 Physical verification of fixed assets

PRIMARY OBJECTIVE

Perform periodic verification of the fixed assets to ensure the accuracy and completeness of the balances in the financial statements

RISK
- Inaccurate or fraudulent recording of fixed assets (Step 1)
- Non-adherence to accounting and reporting requirements and standards (Step 1)

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Completion of a physical inventory of fixed assets is performed at least once every three years with counts documented and differences identified and adjusted after approval by the CFO. *Annual***

REQUIREMENTS

- Regular physical inventories of assets are performed on a rolling basis (at least once every three years) and differences in floor to list and list to floor comparisons are identified. Material differences are investigated to identify the root cause and any adjustments needed are approved by the CFO then recorded.

Link to: Finance Policy

Revenue

20 Management of customer and material master data

PRIMARY OBJECTIVE

Ensure only authorized personnel can create, modify and delete customer and material master data.

RISK

- Transaction with sanctioned parties (Step 1)
- Failure in customer master data creation or maintenance (Step 2, 3, 4)
- Money laundering (Step 2)
- Failure in material master data creation or maintenance (Step 3, 4, 5)
- Unauthorized access, disclosure, modification, damage or loss of data (Step 6)

IMPACT

- Compliance
- Reputational damages
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Countries identify if there is a need for screening for any new customer to validate they are not designated as having a sanctions risks. When required, a sanctions screening is performed and documented locally.** ***Upon Request***
2. **Changes to customer master data are based on approved requests and performed by an authorized user only. Quarterly review and sign-off by the manager responsible for changes to customer master data for a minimum 25 random samples to ensure such changes were based on approved requests and performed by an authorized user.** ***Quarterly***
3. **Annually extract a list of inactive customers and ensure they are blocked / deactivated. Exceptions, if any, are documented and approved by the responsible, identified locally. Annual**
4. **Quarterly verification and sign-off by the responsible manager to ensure only users from customer Master Data Management function have access to change customer master data.** ***Quarterly***
5. **Changes to material master data are based on approved requests and performed by an authorized user only. Quarterly review and sign-off by the manager responsible for changes to material master data for a minimum 25 random samples to ensure such changes were based on approved requests and performed by an authorized user.** ***Quarterly***
6. **Quarterly verification and sign-off by the responsible manager to ensure only users from material Master Data Management function have access to change material master data.** ***Quarterly***

REQUIREMENTS

- Before adding a new customer in countries designated as having a sanctions risk (see Legal & Compliance intranet portal/sanctions), obtain a sanctions screen (or exemption) from local or regional compliance and/or Sanctions Board Approval, when required. Sanctioned entities or individuals cannot be added to the customer master data. There should be an ongoing sanctions screening as defined in the Sanctions and Export Controls Directive: systematically as defined in Symfact and at transaction level considering the defined transactions in scope. (Step 1)
- The addition of a new material and subsequent changes require approval based on a predefined approval process or framework with appropriate supporting documentation. A check is performed to confirm that all required information is completed. (Step 2)
- The addition of a new customer and subsequent changes require approval based on a predefined process with appropriate supporting documentation. As a minimum, a document supporting the identify of the customer is required. One of these examples suffice: Certificate of incorporation or registration, Extract from commercial register, Business license, Tax certificate, DUNS certificate, National ID for individuals. Bank documentation is highly recommended for inclusion of a customer in the customer master data but not mandatory, at a minimum its required when a refund or subsequent change to bank record is to be processed. One of these examples suffice: RIB; IBAN; bank letter of confirmation or bank statement, a copy of canceled check or other acceptable documentation that establishes the customer identity to the bank details. A check is performed to confirm that all required information is completed. Regional specificities to be aligned with Regional IC Director.(Step 2)
- For existing customers, changes to bank information in the customer master data must only be done post execution of the callback process, of which must be documented with a post confirmation via email that the verification call took place. (Step 2)
- Quarterly, a master data change report is run of all creations, modifications and deletions to ensure that all the changes were duly approved and performed by authorized users. If any exceptions are found, they are documented and reported immediately for investigation. Corrective actions are documented and tracked. All exceptions are closed within the locally defined timeframe. As minimum, in SAP the following fields for customer master data should be considered as critical: Customer name, Value Added Tax (VAT), Bank details (as defined above), reconciliation account, account assignment group, payment terms, tolerance group and for material master data: account assignment group, valuation class, price control. Other fields can be added locally above the minimum (Step 2, 5)
- Customer records should be reviewed on an annual basis for activity and any record with no activity for a long period (18 months) should be deactivated, with the exception of Solutions & Products' customers (warranty program). (Step 3)
- Changes to customer and material master data directly in SAP should only be performed by SCs.(SAP only and whenever possible) (Step 4, 6)

Link to: Sanctions and Export Controls Directive (Sanctions and Export Controls Resource Center)

21 Price management

PRIMARY OBJECTIVE

Prevent unauthorized changes to prices, discounts or rebates.

RISK
- Lack of commercial strategy and pricing policy (Step 1)
- Unauthorized commercial commitments and conditions (Step 1, 2, 3)

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Approval per the Delegation of authority of standard prices, discounts and rebates, price changes and exceptions to standard discounts or rebates are reviewed and documented.** ***Upon Request***
2. **Quarterly verification and sign-off by the responsible manager to ensure only users from commercial function as per Delegation of authority / approved Business Service Center users have access to change pricing data.** ***Quarterly***
3. **Quarterly pricing master data change report (including pricing condition modifications) is reviewed and signed-off by the responsible manager. Unauthorized change to the master data is investigated and corrective actions taken.** ***Quarterly***

REQUIREMENTS

- All price determination processes are defined in a written pricing policy and formalized in sales contracts and/or sales orders, compliant with legal requirements as well as fair competition and anti-bribery and corruption laws and regulations. A price list of all products and services are set by pricing, sales and marketing, taking into account different pricing aspects as per pricing policy, including other providers (e.g. transporters, applicators). A complete list, including effective dates, is communicated to the team responsible for updating the list in the system. No backdating of effective prices is allowed. (Step 1)
- Standard discount and rebate structures are defined for different categories of customers. Each discount or rebate type is documented in the company's policy with specific objectives, clear rules of application that were approved by management and supported by local legal/compliance. No backdating of discounts and rebates schemes allowed. (Step 1)
- Exceptions to standard discounts/rebates are specified in accordance with the company's policy and are authorized by the designated approver. (Step 1)
- Price changes are properly approved, accurately reflected in the system and exception reports are leveraged and reviewed before the sale. Corrective actions are duly closed within the process of the company's policy and documented. (Step 1, 2)
- All employees must comply with the Commercial Documentation Directive to ensure all pricing decisions, competitor contacts and sources of market information are properly documented (MCS 02)
- Pricing master data change report available at each region/country is reviewed. (Step 3)

Link to: Anti-Bribery and Corruption Policy, Fair Competition Directive, Commercial Documentation Directive

22 Control of customer credit limits

PRIMARY OBJECTIVE

Grant prior authorization for customers exceeding their credit limit.

RISK
- Unauthorized commercial commitments and conditions (Step 1)
- Poor credit and risk management process resulting in increased bad debt (Step 1)
- Transaction with sanctioned parties (Step 2)

IMPACT
- Compliance
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Prior to shipment, ensure there is an automated or manual check to prevent shipment/ delivery to customers exceeding credit limit (credit block). Approval as per the local Delegation of authority is required to change customer credit limit. *Upon Request***
2. **Letters of credit/guarantees or note acceptance by banks not in the Holcim Bank list are sanction screened and approved by Group Treasury before the release of the goods/services. *Upon Request***

REQUIREMENTS

- Credit line to a single customer (legal entity level) to be approved in accordance with the Group Delegated Authorities (GDA). In case the sale is covered by a security delivered by a third party (letter of credit, stand by letter of credit or a first demand bank guarantee) the amount secured shall be deducted from the risk exposure only if the security is on first demand (confirmed LC/stand by LC/first demand guarantee,...) and issued by a first class bank accepted by Group Treasury . Only in this case, the credit limit/line will be submitted for approval based on the net risk exposure after deduction of the security. (Step 1)
- Credit limit checks must take place for all sales orders. Orders exceeding a customer's credit limit are managed and approved according to an appropriate procedure and local Delegation of authority (DoA). (Step 1)
- No shipments are allowed when customers exceed their credit limit until (Step 1):
- An increased credit limit has been properly approved by delegation of authority and updated in the system.
- The individual order is released following a documented effective approval process to avoid unnecessary disruption.
- All invoices, deliveries, credit notes and orders are computed to calculate the customer balance and to compare it against their credit limit.
- Any practice of bypassing a hold on customer shipments (manual shipment, fictive cash customer account, etc.) are restricted and tracked by exception reports. Corrective actions are duly closed within the process of company's policy and documented.
- If applicable, all letters of credit/ guarantees or note acceptance are issued/confirmed by a bank part of the Holcim Bank List before the release of the goods/services. The acceptance of banks not part of the Holcim Bank list is subject to sanction screening and Group Treasury approval. (Step 2).

Link to: Group Delegated Authorities (GDA), Finance Policy, First class bank accepted by the Holcim Group, Sanctions and Export Controls Directive

23 Matching of sales orders, shipments and invoices

PRIMARY OBJECTIVE

Match and reconcile sales orders, shipments and invoices to ensure proper revenue recognition.

RISK
- Unauthorized or erroneous sales orders and / or shipments (Step 1, 3, 4)
- Unauthorized commercial commitments and conditions (Step 1, 2, 3, 4)
- Inaccurate or fraudulent revenue recognition (Step 1, 2, 3, 4)

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Monthly reconciliation of quantities and correction of any differences identified in the matching of sales order, invoices and shipments, including deviations from weighbridge tolerances, to ensure that all deliveries are invoiced.** ***Monthly***
2. **Weekly (or in line with the locally defined frequency of customers' invoicing) reconciliation by the billing team of unbilled items and resolution within a week.** ***Upon change***
3. **Monthly verification and approval by finance of any sales accrual needed at month-end based on unbilled items.** ***Monthly***
4. **Open sales orders with a planned delivery date in the past (not shipped/ invoiced) are reviewed monthly and resolved on a timely basis.** ***Monthly***

23 Matching of sales orders, shipments and invoices

REQUIREMENTS

- All sales orders, shipments and invoices are recorded in the applications. (Step 1)
- There is a pre-defined tolerance threshold at the weighbridge for dispatched goods. at least annually, weighbridges and measurement equipment are re-calibrated as per local regulations. (Step 1)
- Accuracy of amounts invoiced are checked when manually calculated, or are accurately calculated by the application system using standard programmed algorithms and established terms of sales (unit price, discount and rebates rate). (Step 1)
- Invoices/billing (e.g. quantities, price, discount, rebates, product, customer data) are matched with sales orders, quantities shipped & customer master file information. An automated match is performed between the invoice and order (including all necessary data). (Step 1)
- Any differences are investigated and related adjustments are approved and documented (e.g. returns, redispatch, interco mismatch, cut-off). In addition, any discounts and taxes match the approved parameters in the system from sales order to invoice. (Step 1)
- SAP: All orders shall be processed via SD including any discounts and rebates, i.e. no direct FI bookings. (Step 1)
- There is, at least at month end, a follow-up on unbilled items. The report of unbilled items is reviewed weekly (or in line with the locally defined frequency of customers' invoicing) by the billing team and all the unbilled items are billed within one week from the date they first appear in the unbilled report and within the same reporting month as the delivery. Every month end, the sales manager receives the information, documenting any follow-up action. Finance verifies and approves the need for a possible adjustment entry (e.g. sales accrual) at the end of the month, based on the unbilled items. (Step 2, 3)
- Rules for closure of open sales orders with delivery date in the past must be defined locally in accordance to the sales terms and conditions, but should be resolved at a minimum half yearly. (Step 4)

24 Accounts receivable valuation

PRIMARY OBJECTIVE

Ensure receivable balances are reviewed and provisions are recorded on a quarterly basis.

RISK
- Unauthorized or erroneous sales orders and / or shipments (Step 1, 2)
- Poor credit and risk management process resulting in increased bad debt (Step 1, 2, 3)
- Inaccurate or fraudulent revenue recognition (Step 1, 2, 3)

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Quarterly review and approval by the designated finance person of the provision for bad debt.** ***Quarterly***
2. **At minimum, quarterly monitoring by the Credit Committee of the doubtful account balances.** ***Quarterly***
3. **Recording of write-off approved by the Credit Committee according to the Delegation of authority (DoA).** ***Upon Request***

REQUIREMENTS

The bad-debt provision must consider the risk of debt recoverability at the end of the reporting period every quarter (Step 1, 2):

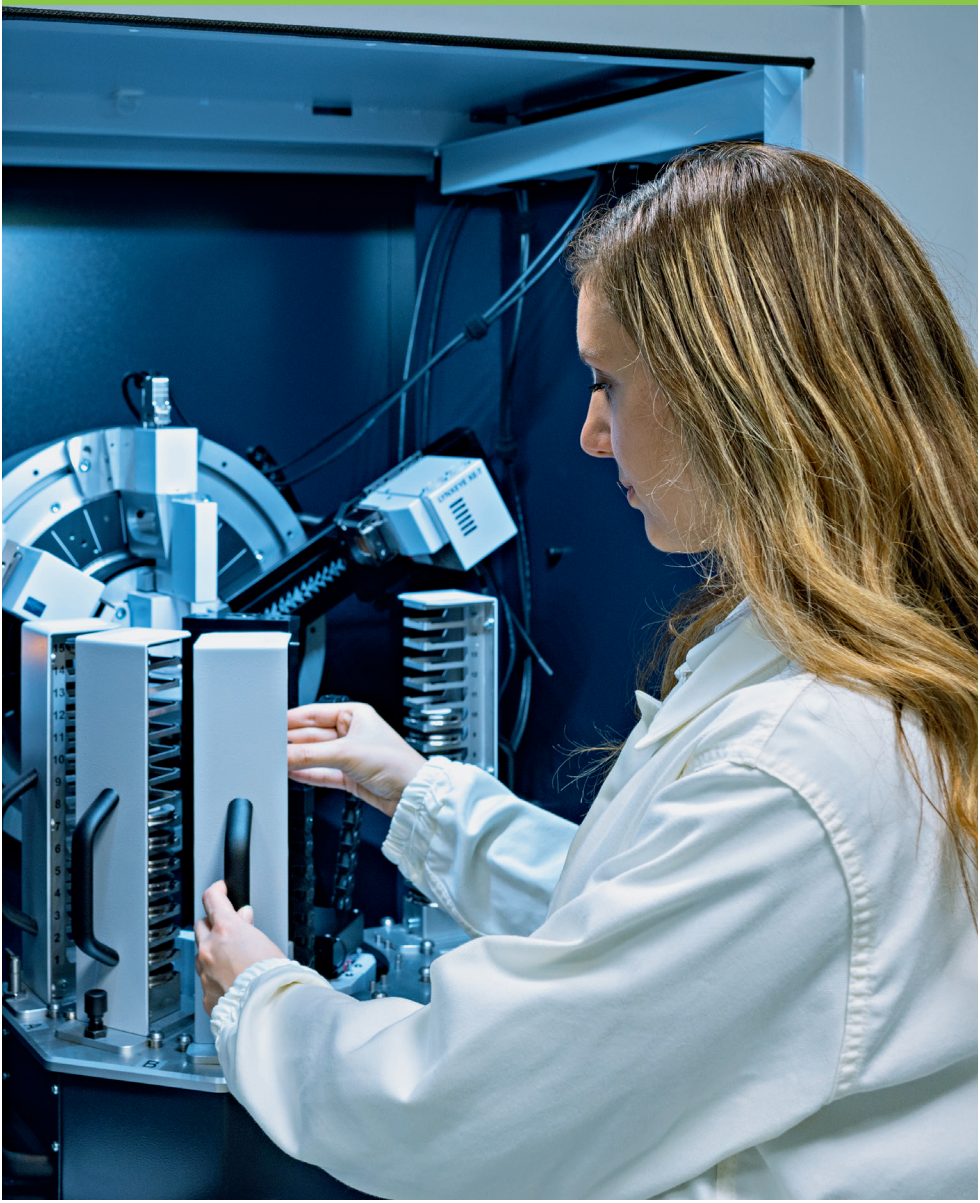
- Quarterly reconciliation of trade balances with the customers must take place, and documentation kept to demonstrate effort to collect the receivables (formal dunning process and exchanges with the trading partner).
- The assessment of the bad debt provision is estimated using an expected credit loss model (ECL). The provision is based on a forward-looking ECL, which includes possible default events on the trade accounts receivable over the entire holding period of the receivable. This method is applicable for all financial receivables including trade accounts receivables, prepaid expenses and other current assets (IFRS 9).
- Any change is clearly documented and justifiable by the Country
- Provisions are reviewed and approved by the appropriate Country finance person and recorded by the designated department.
- The Credit Committee meetings are held regularly(at least quarterly) to monitor the doubtful accounts receivable balances.

Review over specific Accounts Receivables which indicates uncollectibility is considered for write-off. Uncollectibility is evidenced by significant difficulty of debtor, a high probability of bankruptcy or other situations as defined in Holcim Accounting and Reporting Principles (HARP) (Step 3).

- Write-offs are determined by the Credit Committee on the basis of appropriate supporting documents
- Write-offs for amount above a locally defined thresholds approved by the Country CFO.
- If receivables are collected after being written off, the amounts collected should be directly credited on the company bank account and the information provided to Accounts Receivable department.

Link to: Group Delegated Authorities (GDA), Finance Policy

Human Resources



25 Execution of onboarding, offboarding, master data management and transfers of workers

PRIMARY OBJECTIVE

Ensure onboarding, offboarding and worker transfer processes, including employee master data management, exist and cover payroll changes, recovery of assets, system access termination and comply with legal regulations.

RISK

- Lack or ineffective HR management process (for example onboard, offboarding, worker transfer process) (Step 1, 2, 3)
- Failure in employee master data creation or maintenance (Step 4)
- Unauthorized access, disclosure, modification, damage or loss of data (Step 5, 6)

IMPACT

- Compliance
- Reputational damages
- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Signing, by the employee and the company, of employment contracts or hiring documentation for all employees, including a Compliance Reference Check for Senior Leaders Group or Country Executive Committee positions.** ***Upon Request***
2. **Notification to IT by Human Resources or the business to request termination of access from all systems before the last working day of user leaving the company. Confirmation by the Human Resources that all assets were recovered from terminated employees and employee system was deactivated prior to final payroll payments.** ***Upon Request***
3. **Quarterly verification by Human Resources and cost center responsibles that the headcount report is accurate (only own active employees, proper coding and classification).** ***Quarterly***
4. **Quarterly review and sign-off by the control owner for changes to employee master data for a minimum 25 random samples to ensure such changes were based on approved requests and performed by an authorized user.** ***Quarterly***
5. **Monthly validation of the employee movements (hire, transfer and departure) recorded in the Employee Master Data and check the data consistency between employee data in the local system and SuccessFactors master data.** ***Monthly***
6. **Quarterly verification and sign-off by the control owner to ensure only authorized users from the Human Resources department have access to manage employee master data in SuccessFactors and employee data in the local system.** ***Quarterly***

For countries using systems other than SuccessFactors for employee master data management, equivalent requirements and controls (4, 5 and 6) must be in place.

REQUIREMENTS

- Employment contracts or hiring documentation exist for all employees and are signed, as per Group Delegated Authority (GDA) or Delegation of Authority (DoA). Employment contracts (if applicable by law) or hiring documentation with all new employees refer to the Code of Business Conduct (CoBC) and indicate that disciplinary measures can be taken on the ground of this document in case of a breach. For all new appointments to a Senior Leaders Group (SLG) or Country Executive Committee position, the appointing manager must request a Compliance Reference Check from the relevant Region Compliance Officer (or delegate) and for Group level appointments from Group Compliance. (Step 1)
- A process is in place for Human Resources (HR) administration to be informed of all moves of both employees and temporary workers paid through payroll in a timely manner, including on-boarding, off-boarding and changes of position. (Step 2)
- For people changing positions or leaving the company, there is a process to monitor the recovery of all company assets by notifying relevant departments of the change and obtaining confirmation that the assets were recovered. This includes a confirmation from the IT Department that the employee access is deactivated. (Step 2)
  - User termination process is agreed between the Human Resources / Business and the IT function - Human Resources/ Business notifies IT on or before the last working day of the user who is leaving the company (e.g. end of contract, resigned, terminated etc.) requesting termination of access from all IT systems
  - Where the termination process is not automated, a notification is received back from IT in a timely manner confirming that all IT system access is terminated (within 5 working days from the requested date)
- All employee departures follow a strict written procedure ensuring that all legal requirements have been respected (in particular in case of lay-off) and all payroll related payments have been made to the employee, once all company assets have been retrieved (only applicable if in compliance with local labor legislation). (Step 2)
- At least quarterly, employee headcount is reviewed and validated for accuracy between Human Resources and cost center responsibles, to ensure that: 1) all own employees on the payroll are actively employed as per the latest contractual situation, 2) employment status (i.e. active, leave, etc.) and the classification of employee is accurate, and 3) the payee is coded to the correct cost center. Any discrepancies found should be resolved within 30 days. (Step 3)

25 Execution of onboarding, offboarding, master data management and transfers of workers

REQUIREMENTS

Human Resources System Master Data Management:

- After the go-live in SuccessFactors, an Employee Master management process that defines roles, responsibilities and rules for employee data management must be in place and reviewed quarterly. In addition to the fields defined as critical and mandatory in SuccessFactors (procedure Master Data Completion Governance), each HR entity must formally define its mandatory and critical fields for employee master data, in line with the local regulations and business requirements. (Step 4)
- The addition of new employee data and subsequent changes require appropriate approval based on an employee change request with supporting documentation. Each HR entity must identify mandatory supporting documentation as per local regulations. Employee records should be accurately and completely recorded within 30 days of the event. A check is performed to confirm that all required information is completed and accurate. Changes to Employee Master Data in SuccessFactors must be processed according to the standard Group HR definitions and across the life cycle changes of an employee (e.g. hire, job change, termination, etc).(Step 4)
- Quarterly, an employee master data change report is run of all creations, modifications and deletions to ensure that all the changes were duly approved and performed by authorized users. If any exceptions are found, they are documented and reported immediately for investigation to the Group HRIS team. Corrective actions are documented and tracked. All exceptions are closed within the next 2 weeks. (Step 4)
- At least monthly, the entity Human Resources team must reconcile the SuccessFactors and employee data in the local system to ensure data consistency (procedure). Review of the employee movements (hire, transfers and departure) is performed to ensure that they are properly recorded in the local employee data and SuccessFactors. Discrepancies are to be corrected within 30 days (Step 5)
- Only authorized users from the Human Resources department have access to manage employee master data in SuccessFactors and employee data in the local system for employee data management (procedure). (Step 6)

For countries using systems other than SuccessFactors for employee master data management, equivalent requirements and controls (4, 5, 6) must be in place.

Link to: Group Delegated Authorities (GDA), Group Human Resources Policy, Compliance Negative Reference Check procedure, HARP 6.11.1 Personnel FTE, SuccessFactors Security Roles, SuccessFactors Security Template

26 Payroll

PRIMARY OBJECTIVE

Review, validate and reconcile payroll before and after processing every month.

RISK
- Non compliance with local HR laws and regulations (Step 1, 2, 3)
- Error in payroll process or unauthorized employee benefit (Step 1, 2, 3)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Monthly payroll approval by Payroll Team for reasonableness and data accuracy prior to processing. *Monthly***
2. **Reconciliation by Payroll Team of total payments to the payroll journal after payroll processing. *Monthly***
3. **Approval by the cost center responsible that the employee being charged to their department are correct. *Quarterly***

REQUIREMENTS

- Approval prior to processing payroll (Step 1):
  - Balancing routine control: For manual and mass uploading imports, the payroll manager should perform data accuracy controls (e.g. verify that the input of total hours worked received from the manager matches with the total hours worked indicated in the payroll system; verify that the total amount of bonus received from Human Resources matches with the total amount in the payroll system). In case of Payroll system integration with any other system, interface should ensure data approval from the source.
  - When bonus or any other payout is processed (with or without payroll), secondary approval should be performed to ensure accuracy of payout, both at individual and total amount to be paid.
  - Analytical review comparing one month to another justifying variance (if any) is performed before bank transfer (analytical review covers payroll exception reports to identify unusual amounts e.g. negative value check, zero value check, significant increase between two months)
- Reconciliation after processing payroll: For each payroll, the total payment issued (treasury account) is reconciled with the payroll journal in order to check that amount paid to employees matches with the amount calculated by payroll department.(Step 2)
- At least every six months (e.g. during Salary & Bonus review and Budget, MTP or Forecast cycles), or more frequently if risk is identified as high, cost center responsible must validate that the own employee cost being charged to their department is correct (total employee cost). High risk countries are identified by the Regional HR Director in coordination with the Regional Internal Control responsible. Any discrepancies found should be resolved within 30 days.(Step 3)

Link to: Group Human Resources Policy

27 Compliance with payroll and local labor laws

PRIMARY OBJECTIVE

Ensure payroll and employment practices are compliant with local labor laws. Work permits and work contracts are in place, checked, and up-to-date at all times.

RISK
- Non compliance with local HR laws and regulations (Step 1, 2, 3)
- Error in payroll process or unauthorized employee benefit (Step 1, 2)

IMPACT
- Reputational damages
- Financial losses

CONTROL & FREQUENCY

1. **Annual review and assessment by Human Resources of key payroll, employment practices, employee liability and laws to ensure compliance. In case of non compliance, notification to finance, legal and compliance to assess any financial impact / provisions / disclosure.** ***Annual***
2. **Employee data in the local system are timely updated in the event of a change.** ***Upon Change***
3. **Quarterly review, follow up and closure of open compliance actions related to local labor laws and regulations.** ***Quarterly***

REQUIREMENTS

- The Human Resources (HR) department should have an updated information / checklist (of applicable local labor laws and regulation). Annual assessment should be performed to ensure compliance. Any identified gaps are reported, and followed up for timely action. In case of non-compliance with the local regulation, a risk analysis is performed and communicated to the Finance, Legal and Compliance departments to determine the potential needs for provisions, disclosures or actions to achieve compliance. (Step 1)
- Employee data in the local system is maintained up to date. Changes are timely updated in the employee files / master data upon notification. (Step 2)
- Actions related to any non compliance are recorded and followed up quarterly to ensure they are timely closed. (Step 3)

Link to: Group Human Resources Policy

28 Employee pension and benefit plans

PRIMARY OBJECTIVE

Ensure employee pensions and post-employment benefit plans are defined according to Group policies and local labor laws with proper calculation and recording.

RISK
- Error in payroll process or unauthorized employee benefit (Step 1, 2)
- Pension fund insufficiently capitalized, mismanaged or with insufficient transparency regarding future obligations (Step 1, 2)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Any new plans, amendment or de-risking project of current plans must be communicated by the sponsor (local company) to Pension and Benefits Governance Team and approved as per Group Delegated Authority following recommendation of the Pension and Benefits Governance Team. Annually, Pensions and Benefits team to update the list of all pensions and post-employment benefit plans and validate with Group Pension and Benefits Governance Team that they are managed in line with the Group Pension & Benefits Directives. *Annual***
2. **Twice per year, CFO (or designee) should ensure that pensions and post-employment benefit plans are correctly valued within the due date communicated in the Group Accounting, Reporting, Consolidation and Controlling pension instructions. CFO (or designee) should provide a sign-off for the actuarial results, at least annually, in the Group actuary tool (RA tool) and ensure that inputs and outputs are correct and proper accounting entries are booked. A reconciliation of the actuarial data is performed by CFO (or designee), with the support of the Group actuary, between the Group actuary tool and the consolidation tool. *Half year***

28 Employee pension and benefit plans

REQUIREMENTS

The Group Pension & Benefits directive defines the scope and objective together with the rules for managing the plans. Group Accounting, Reporting, Consolidation and Controlling (ARC) issues detailed instructions for reporting of post-employment defined benefits plan. (Step 1, 2)

- Section 4.1 of the directive sets the rules for design of pension plans and other post-employment benefits which should be in accordance with the local regulations and market practices.
- Approval rules to be followed for defined in section 4 for each activity (e.g. closing and freezing pension plans, de-risking liability management, de-risking investment strategy, employer funding contribution etc.)
- Reporting for post-employment defined benefit plans should follow the process as per instructions from Group Accounting, Reporting, Consolidation and Controlling. Actuarial methods and assumptions to be used should be aligned with the instructions
- Reporting should be updated in AON tool - RA as per the instructions for the relevant plans. The local actuary should upload the information related to benefit plans together with actuarial report. The CFO (or designee) should review and sign-off the results and accounting entries. CFO (or designee) should have control over inputs (mainly employee data), and then outputs (analytic review of the main parameter and final results) in addition to the control performed over the assets valuation.
- The Group oversees the management of its pension plans through the Pension and Benefits Governance Team (PBGT). This interdisciplinary team including finance, human resources and legal specialists acts as a center of expertise in all issues relating to pension and other post employment benefits and makes recommendations to Group management. The Sponsor (local company) has to inform the Pension and Benefits Governance Team of any project of new plans or amendment of current plans and request approval as per Group Delegated Authorities (GDA).

Link to: Group Delegated Authorities (GDA), Group Human Resources Policy, Finance Policy, Group Pension and Benefits Directive, HARP section 4.5.2.5, RA User Guide

Expenditure

29 Management of supplier master data

PRIMARY OBJECTIVE

Ensure only authorized personnel create, modify and delete financially relevant vendor data.

RISK

- Failure in vendor masterfile maintenance: error, fraud, duplicate, etc. (Step 1, 2, 3)
- Unauthorized access, disclosure, modification, damage or loss of data (Step 1, 3)

IMPACT

- Compliance
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Changes to supplier master data are performed by an authorized user and based on an approved request. Quarterly review and sign-off by the manager responsible for changes to supplier master data for a minimum 25 random samples to ensure such changes were based on approved requests and performed by an authorized user.** ***Quarterly***
2. **Annually the master data quality check is performed and duplicate, inconsistent and inactive supplier accounts are blocked /deactivated. No exceptions are permitted.** ***Annual***
3. **Quarterly verification and sign-off by the responsible manager to ensure only users from MDM function have access to change supplier master data.** ***Quarterly***

REQUIREMENTS

- A supplier master data management process that defines roles, responsibilities and rules is in place and reviewed when required. (Step 1, 3)
- Duplicate check is performed before a new record is created. Duplicate records are not permitted. Each entity should formally define its mandatory and critical fields in SAP/Local ERP, in line with the legal and business requirements. The list should include as minimum legal name, bank details, incoterms, reconciliation account (General Ledger) and control data (Goods Receipt-based invoice verification).Other fields can be locally added above the minimum. (Step 1)
- The addition of a new supplier requires appropriate supporting documentation. A check is performed to confirm that all required information and documents are complete.(Step 1)
- For existing vendors, changes to bank account details must only be done post execution of the callback process using the registered contact information in the master data. The call must be documented with a post confirmation via email. The changes are supported by appropriate approval based on supporting documentation. In addition to the supplier request for change, any one of the following supporting documentation are accepted: RIB; IBAN; bank letter of confirmation, cancelled cheque with printed vendor name or bank statement. Any other mechanism for supporting documents for bank changes must be approved by the Group Internal Control with the agreement of Group Treasury and Group Compliance.A check is performed to confirm that all required information and documents are complete.(Step 1)
- Quarterly, a master data change report is run of all creations and modifications to ensure that all the transactions were performed by authorized users based on approved requests and documents. (Step 1)
- If any exceptions are found, they are documented and reported immediately for investigation. Corrective action is documented and tracked. All exceptions are closed in a timely manner (locally defined) (Step 1)
- Supplier records are to be reviewed on an annual basis for data quality (duplicate check, tax code check, bank account check, mismatch in the supplier and bank account country and inactive suppliers for more than 18 months) and are deactivated or blocked for payment and purchase with the exception of Solutions & Products' suppliers (warranty program). Suppliers identified as part of the procurement supplier reduction strategies are to be deactivated and flagged for deletion. (Step 2)

Link to: Procurement Policy

30 Supplier qualification

PRIMARY OBJECTIVE

Screen and qualify suppliers before their addition to the supplier master data and manage supplier performance.

RISK
- Ineffective or unethical vendor selection process (incl. TPDD process) (Step 1, 2, 3)
- Transaction with sanctioned parties (Step 1)

IMPACT
- Compliance
- Reputational damages
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Screening of potential suppliers by Procurement (or designee) based on the criteria required by Procurement, Sustainability, and Compliance including Sanctions and Third Party Due Diligence, must occur prior to entering into a transaction or adding a supplier in the supplier master data or approved supplier list. *Upon Request***
2. **Review of supplier performance by Procurement must occur for critical and strategic critical criteria (including suppliers with high ESG impact) with suppliers not meeting the requirements being flagged as disqualified until action plans are completed, or the supplier is blacklisted if there are ongoing issues. *Annual***
3. **Supplier qualification must be updated at least on annual basis for critical and strategic suppliers (including suppliers with high ESG impact). *Annual***

REQUIREMENTS

- There are clear rules based on purchasing categories to identify vendors that are required to go through a qualification process. Qualification is performed in line with the Code of Business Conduct for Suppliers, Data Universal Numbering System (DUNS) requirements, and certification such as International Organization for Standardization (ISOs). (Step 1)
- All service suppliers that represent the company to a government agency, official or owned-enterprise to be screened compliant with the Third Party Due Diligence Directive (TPDD) before inclusion in the supplier master data. (Step 1)
- Before adding a new supplier in countries designated as having a sanctions risk (Legal & Compliance intranet portal/sanctions), obtain a sanctions screen (or exemption) from local or regional compliance. Sanctioned entities or individuals cannot be added to the supplier master data. Sanctions and Export Controls Directive (Step 1)
- Supplier qualification should include the following: Health and Safety, Human Rights and Labor, Environment and Bribery and Corruption criteria, as defined in the Sustainable Procurement Management Standard, the Sustainable Procurement Directive, Commercial (financial health of the supplier); Technical (goods and services as defined by category teams) and Management & Tracking to on-going performance evaluation linked to a Claim Management and Consequence Management processes. (Step 1,2)
- In case of poor supplier performance or repeated unsolved claims, the Category Manager agrees with the supplier on a corrective action plan; if this corrective action plan is not followed or not efficient, the supplier is blacklisted. (Step 2)
- During the ongoing qualifications, supplier performance is periodically assessed for at least critical and strategic criteria (including suppliers with high Environmental, social, and governance (ESG) impact) and any supplier that does not meet the requirements must be flagged as disqualified and consequent management applied (ex. replacement). (Step 2,3)

Link to: Code of Business Conduct for Suppliers Procurement Policy, Third Party Due Diligence Directive (TPDD),Sanctions and Export Controls Directive, Sustainable Procurement Directive, Shipping Directive, Sustainable Procurement Management Standard and Legal & Compliance intranet portal/sanctions

31 Three-way match, two-way match and direct vendor invoices

PRIMARY OBJECTIVE

Reconcile purchase orders, receipts and invoices (3-way match) or approve 2-way match or vendor direct invoices to clear invoices for payment.

RISK

- Fraudulent or incorrect purchase order (Step 1, 2, 3, 4)
- Lack of control (quality and quantity) of goods and services received (Step 3)

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Approval in the system by the designated approver according to the Delegation of authority of all purchase requisitions or purchase orders (depending on system design).** ***Upon change***
2. **Verification and correction of exceptions by the designated responsible (business or procurement) to the three-way match report and approval according to the local Delegation of authority if the exception is above the locally defined threshold.** ***Upon change***
3. **Approval by the requisitioner or other designated approver per the local Delegation of authority of any 2-way match invoices to confirm that the amount and workflow are correct and goods or services are received.** ***Upon change***
4. **Approval by the designated approver per the local Delegation of authority in the system of any vendor direct invoices to confirm that the amount and workflow are correct and goods or services are received.** ***Upon change***

REQUIREMENTS

Purchases using purchase orders (Step 1, 2):

- Purchasing instruments (purchase request, purchase orders, framework orders or contracts) are approved according to country, regional and Group delegations of authority (involving legal and financial departments when required) prior to entering into a commitment with the supplier. (Step 1)
- Supplier invoices are only cleared for payment after the system automatically matches the purchase order, receipts and the supplier invoice (3-way match) or purchase order and an approved invoice (2-way match). (Step 1)
- Discrepancies between the invoice, purchase order (PO) and receipt are formally identified and the system blocks the payment process if the discrepancy exceeds the locally defined threshold. (Defined thresholds must be documented & approved by local Delegation of authority (DoA). (Step 2)
- An exception report (exception to 3-way match) is distributed regularly for verification and resolution. Only when the exceptions are cleared and properly explained can the payment be made. If discrepancies exceed a defined threshold, payment requires approval as per Delegation of Authority. (Step 2)

Purchases using vendor direct invoices (if applicable) with locally defined criteria (Step 2,3,4):

- Any vendor direct invoices (SAP FI invoices) which qualify for payment without a PO are entered into the system and are sent into a workflow immediately for review and approval according to local Delegation of authority (DoA). Vendor direct invoices are discouraged and must be limited. Once the responsible employee reviews the invoice to confirm the amount, that the goods or services were received and approved, the invoice is cleared for payment.

Link to: Procurement Policy

32 Payment processing

PRIMARY OBJECTIVE

Approve payments/cash disbursements in accordance with local and Group Policies and Directives.

RISK
- Unauthorised or erroneous processing of supplier payments (Step 1, 2, 3)
- Corruption and bribery (Step 1, 2)
- Transaction with sanctioned parties (Step 1)
- Money Laundering (Step 1)

IMPACT
- Compliance
- Reputational damages
- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Approval according to the Group Delegated Authorities and related directives, and local Delegation of authority of all payments and cash disbursements prior to payment.** ***Upon Request***
2. **Expenditures falling in the Gift, Hospitalities, Strategic Social Investments, Sponsorship and Donations, entertainment and travel and expense categories are identified through the accounting system. Payment carried out in contradiction to the Gifts, Hospitality, Entertainment and Travel or Sponsorship and Donations Directives are rejected.** ***Upon Request***
3. **Monthly review and approval by the designated finance person of the accounts payable subledger accounts and the aging report to examine unusual balances and take corrective actions.** ***Monthly***

REQUIREMENTS

- Payments / cash disbursements are approved according to the local and Group Treasury Directive, Group Delegated Authorities (GDA) and local Delegation of Authority prior to actual payment. (Step 1)
- Payments related to transactions that did not go through the purchase order (PO) or Direct Invoice (FI) process are authorized on the basis of appropriate supporting documents and according to local Delegation of Authority (DoA) prior to actual payment. Following are the acceptable list of supporting documents for manual payment requests: Invoice including IBAN / Bank details, Agreement/ contract including IBAN / Bank details, Official document of the local authorities including IBAN / Bank details, Official online registry of Bank detail / IBAN verifiers (e.g. tax office, or companies registry). Where they exist, countries will comply with local regulations. Bank details must be authenticated based on a trustworthy and independent (other than the one provided by the requestor) source of information (two-factor authentication) (Step 1).
- The payment process ensures that distinct persons are in charge of the following tasks: 1) approval for payment (persons signing the check or issuing payment by bank transfer) and 2) accounting (preparation of bank journal entries). Disbursements should be processed by a member of staff independent from the receipt or matching of invoice process. (Step 1)
- Payments to suppliers that represent the company to government agencies, officials or owned-enterprises have been approved under the Third Party Due Diligence Directive (TPDD) before payment can be made. (Step 1)
- Sponsorship & Donation payments or any payment made directly or indirectly to public official without expecting any consideration in return must be reviewed by Compliance and authorized according to local Delegation of Authority (DoA), the Group Delegated Authority (GDA) and the Social Initiatives Directive. (Step 1)
- All business trips require appropriate authorization and controls, to be adhered by both the line managers and employees. The local travel policies shall include an approval system and process in accordance with Travel and Events policy.(Step 1)
- Incorrect payments: A process must be in place to prevent incorrect payments (e.g. use of a report to check duplicate payments, stamping invoices as paid when the payment is issued or other automatic system control). (Step 1)
- Payments made as marketing gifts, hospitalities, entertainments and travels for third parties above the threshold defined by countries, and for public officials, have been approved according to rules defined in Gifts, Hospitality, Entertainment and Travel (GHET) Directive. No reimbursement for cash payments made as GHET is made. (Step 1,2)
- Country CEOs' expenses are to be controlled and approved by the country CFO. If not approved directly in the ERP, the offline (email) approval has to be attached in the local approval system (Step 2)
- In connection with the month-end closing, the accounts payable subledger is reviewed to examine unusual balances (e.g. old balance, debit amount, incorrect currency rate etc.). Debit balances within the Accounts Payable (A/P) subledger are reviewed and justification is checked for (e.g. credit notes, advance payments). The follow-up actions are described and are monitored in the following month.(Step 3)

Link to: Group Delegated Authorities (GDA), Travel and Events Policy, Third Party Due Diligence Directive (TPDD), Group Treasury Directive, Strategic Social Investment, Sponsorship and Donations Directive, Gifts, Hospitality, Entertainment and Travel (GHET) Directive and HARP 3.2.1.2.25 Other Cost Center Expenses, CAPEX Directive

33 Accrual for expenditures not invoiced

PRIMARY OBJECTIVE

Ensure that all accruals for expenditures are properly recorded in financial statements in the correct period.

RISK
- Inaccurate or fraudulent recording of expenditure and accruals (Step 1, 2, 3)

IMPACT
- Errors in financials

CONTROL & FREQUENCY

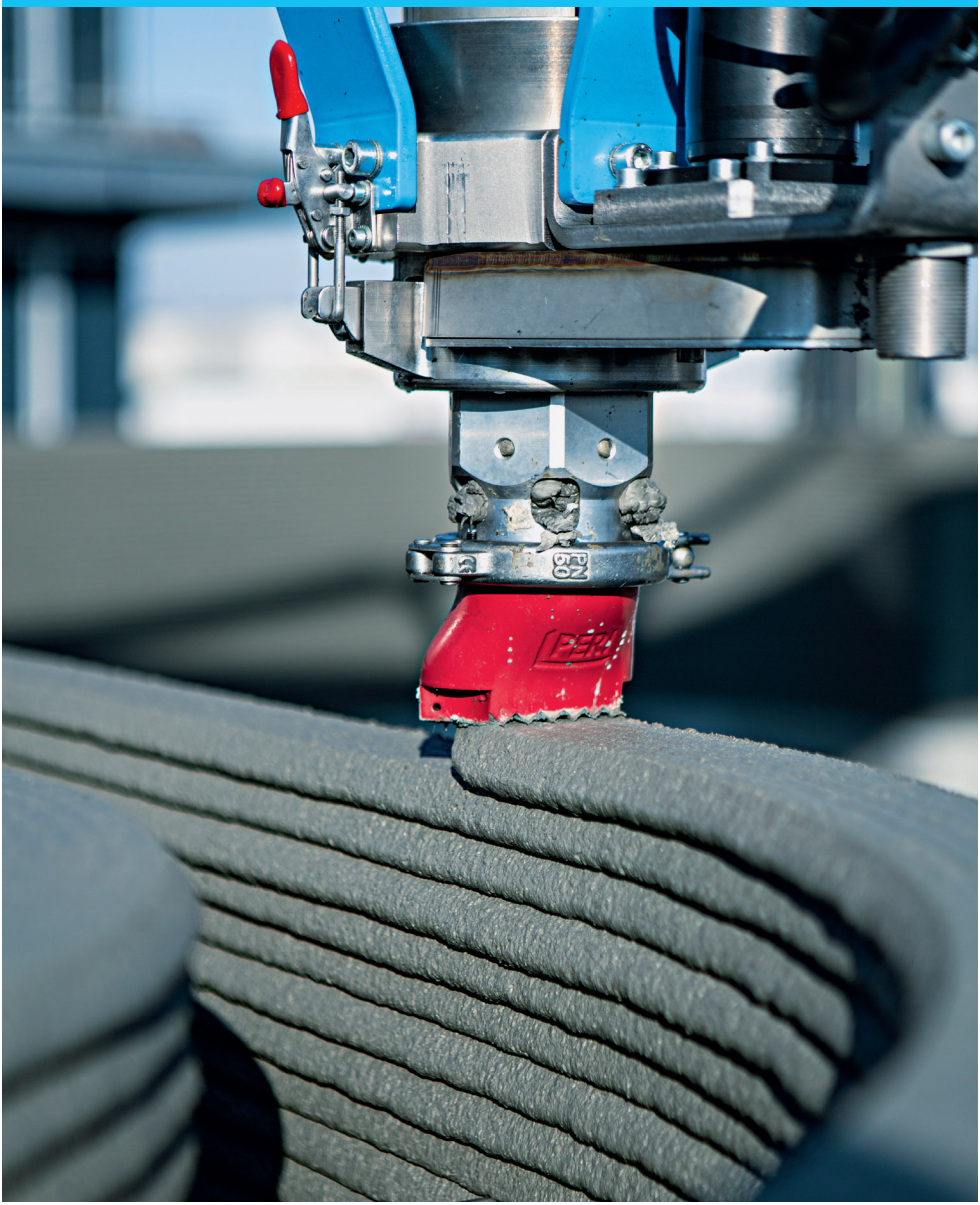
1. **All goods receipts (GR) and services receipt (SR) should be recorded before the month end by the responsible locations. Purchasing manager (or designated) should verify that there are no unrecorded goods receipts or service receipt at the month end for the goods and services received as per the Purchase Order. *Monthly***
2. **Goods Receipt and Invoice Receipt account (or equivalent system account) should be cleared monthly (ongoing) before month end closing by the designated person (business or procurement). *Monthly***
3. **Accruals are booked monthly by the accounting function for all purchases and expenses with pending invoices. Any adjustment to the accruals needs to be approved by the appropriate Financial responsible. *Monthly***

REQUIREMENTS

- There should be a process to review open purchase orders to detect unrecorded goods and services received. Open purchase orders for which the delivery date has passed should be monitored and purchase orders with open quantities that are no longer needed are closed. (Step 1)
- All goods receipts or services rendered (meeting all specifications e.g. quantity, quality) and the corresponding vendor invoices should be timely recorded in the system. If the goods or services are received but the invoice is missing, an accrual is created in the application. The accrual is reviewed for reasonableness on a monthly basis by the Purchasing Manager. (Step 1)
- In SAP GR IR clearing account is an intermediary clearing account for goods and invoices in transit. It represents Goods Receipt and Invoice Receipt (GR/IR) Account. It's a balance sheet account therefore will have a balance at the end of the period. Goods Receipt and Invoice Receipt differences should be reconciled by identifying the difference in the account (missing corresponding invoice or goods receipt). The Goods Receipt and Invoice Receipt ageing should also be reviewed to ensure items are timely cleared. (Step 2)
- For direct purchases (FI Invoice), the responsible department should inform the accounting department before month-end for the invoice not received / recorded. The accounting department reviews the invoices that are missing to determine which expenses should be accrued for proper cut-off. The completeness of the accrual of rendered services and received goods is then validated through a comparison of costs to budget, where applicable, and by reviewing open purchase and service orders (if complete review is not possible, certain thresholds based on budget can be defined locally). (Step 3)
- Follow-up: Old accrual entries which were not offset by the system are followed up monthly and cleared by the Purchasing Manager. Any adjustment related to current month accrual is posted by the Accounting personnel and reviewed by the appropriate Financial responsible. (Step 3)

Link to: Finance Policy

Inventory



34 Physical stock take of spare parts, materials and volume reconciliations

PRIMARY OBJECTIVE

Perform physical stock take of spare parts at least annually and materials at least monthly to ensure that the records reflect the correct descriptions, quantities, and values.

RISK

- Inaccurate or fraudulent recording and tracking of inventory (Step 1, 2, 3, 4)
- Inappropriate physical storage protection and lack of organization for inventories (Step 1, 2, 3, 4)
- Inefficient spare parts management (Step 1, 2, 3, 4)
- Unreliable production data and reconciliation process (Step 3)

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Physical verification of spare parts is conducted annually (or by rotation throughout the year) with counts documented and discrepancy, if any, approved and adjusted according to defined requirements. *Annual***
2. **Physical verification of materials is conducted monthly with appropriate measuring equipments and method by stock owners with counts documented and discrepancy, if any, approved, adjusted and documented according to defined requirements. Any discrepancy over 5% for materials need to be investigated and documented with justifications. Finance function participates in the physical verification process as observer at least half-yearly. *Monthly***
3. **An end-of-month production data reconciliation is performed by the Production manager (or delegated person) as per the defined requirements. Finance/controlling verifies the stock reconciliation process locally performed in the plant and when necessary, applies adjustments to the financial statements according to defined Delegation of authority. *Monthly***
4. **Annual independent full stock take of materials (measurements made by dedicated and skillful team of non-stock owner, e.g. 3rd party service, other functions within the company) is performed with differences identified, approved and adjusted. *Annual***

REQUIREMENTS

Regular physical stock takes of spare parts and materials are organized by the plant team with participation of the finance team and performed according to defined procedures.

SPARE PARTS (Step 1)

1. Preparation of physical inventory

- The plant procedure for stock-taking which describes scope, objective, resources and timeline is available and applied.
- The scope of inventory stock count includes capitalized spare parts, parts with zero/ minimum values (e.g. obsolete parts written-off but still in the plant) and off-site inventories. It excludes consigned stocks for customers and suppliers.
- Movement of parts are stopped or controlled during the stocktaking (reception, issue, return etc.).

2. Stocktake

- Stocktaking is made under adequate supervision.
- Count sheets to be used for the stock-take do not show the quantity recorded in the system (blind count).
- Stocktaking process identifies items that exist but are not recorded and items that are recorded but do not exist (i.e. floor to listing and listing to floor).
- Obsolete items are identified during the stocktaking.

3. Frequency

The stock take of spare parts is to be performed at least yearly. In case full scope stocktake of spare parts is not performed at the year end, monthly or quarterly cycle counts are organized and ensure that all spare parts were included in the yearly stocktake process.

4. Roles and Responsibilities

- The site manager (or designated person) validates and communicates the stocktake planning to all stakeholders. He is responsible, as per local DoA, of the review and approval of the stock-take and of the proposed adjustments.
- The functional manager (based on stock nature) is primarily responsible for the organization and performance of the stock-take. He is responsible to sign-off stock-take results and proposes adjustments in case of physical differences to the site manager.
- The financial controller (or independent designee when necessary) ensures the reliability of the work done, including on-the-field independent observation as part of the count team. He/ she is also responsible for the inventory reconciliation along with the functional manager and when necessary, records adjustments to the financial statements according to defined Delegation of authority (DoA).

5. Follow-up on stocktaking results

- A double count is performed in case of quantity discrepancies for above 5% discrepancy per material (specify by business line)
- Codification, description and label of stocks are checked and updated if needed.
- Stock taking results are reconciled with the data from the inventory ledger by independent people (not those in charge of inventory management).
- This reconciliation is reviewed by the warehouse manager and the finance controller.
- After reconciliation and approval, adjustment entries are recorded in ledgers.
- Discrepancies are analyzed to identify their sources and implement corrective actions.

34 Physical stock take of spare parts and materials and volume reconciliations

REQUIREMENTS

MATERIALS (Step 2, 4)
Materials include raw material, fuel, semi-finished and finished goods

1. Preparation of physical inventory

- There is a layout map to show the scope of the stock take. Off-site stocks are included.
- The stock take planning is validated by the plant manager and communicated to all stakeholders.
- Movement of goods are stopped or controlled during the stocktaking (reception, issue, return, etc).
- Date & time of measurements have to be recorded.
- Calculating formula should be established & declared.
- All the measured figures must be reconciled from the time & date of the measurements to the end of the month at 24h00.

2. Stock take

- Stocktaking is made under adequate supervision.
- Count sheets to be used for the stock take do not show the quantity recorded in the system.
- Stocktaking process identify materials that exist but are not recorded and materials that are recorded but do not exist (i.e. floor to listing and listing to floor).
- Obsolete materials are identified during the stocktaking.

3. Specific matters

- Measuring methods and instruments must be optimized at the maximum to ensure the reliability of the measures.
- Regular calibration of the dosing equipments and weighing devices according to defined schedule.
- Make all the bulk material heaps to regular geometrical shapes as much as possible.
- Bulk density in loose and compact form of all bulk materials should be measured and agreed. Each stock loose or compacted will use the corresponding density.
- Prior to the verification, production manager and mining engineer should certify the geometrical shape and the zero levels of all the major heaps.
- For all bulk materials, the total stock taken into account should include the 'live' and 'dead' stocks.

4. Frequency

- The raw materials & semi finished and finished goods stock take is performed by Production monthly. At least once per year, the stock take should be performed by an independent expert (eg. 3rd party surveyor or other functions when necessary). Third party survey is mandatory if 1) there is local legal requirement 2) business has challenge to ensure adequate physical inventory due to lack of skills/tools/ internal resources.

5. Roles and responsibilities

- Production (stock owner) is primarily responsible for the inventory planning & organization of the stock take to ensure completeness of stock take locations as well as to provide competencies, methodology and tools for the stocktake team.
- Production (stock owner) is also responsible to measure bulk density, calorific value and moisture content at reception and final usage.
- Production team performs the stock take and signs the stock take report. The Production manager (or designated person) and Quarry Managers are responsible to measure physical materials stocks and to propose adjustment of the production figures differences (physical vs.TIS/SAP/JDE).

REQUIREMENTS

- Plant Managers and Manufacturing Directors or Business Line Manager, as per local DoA, are responsible to review and approve production and stock adjustment proposals.
- Financial controller (or independent designee when necessary) ensures reliability of the work done. Finance/ Controlling (or independent designee when necessary) participates on the stock measurement monthly. Finance/ Controlling must participate on the field as part of the count team at least half yearly. The Financial controller is overall responsible for the compliance and reliability of the stock reconciliation process locally performed in the plant and when necessary, records adjustments to the financial statements according to defined Delegation of authority (DoA).

6. Monthly stock reconciliation (Step 3)

- An end-of-month production data reconciliation is performed by Production manager (or delegated person).
- Stock reconciliation is done between all semi-finished / finished goods stock measured values, products delivered, materials received, and production / consumption figures for the current month. Reconciliations should be performed on a dry basis for semi-finished and finished goods, on a wet basis for the other materials (raw materials).
- The following parameters cannot be adjusted and must be considered as fixed: Semi-finished and finished goods tonnages (Shipments, deliveries and physical measures of stocks), total operating hours for the month for each semi-finished and finished goods manufacturing equipment.
- All material physical quantities from stock take inventory are cross-checked with stock information in the data system (TIS and other systems) by independent people (not those in charge of material stock take).
- Discrepancy(ies) between the measured physical stock and stock information in the data system (ERP) for all physical stocks and before proceeding adjustment of production inputs, reliability of the information system, accuracy of stock take and output of the manufacturing lines for the month must be analyzed first. A double count is performed in case of quantity discrepancies above 5%. No adjustments to be made in data system (TIS / SAP / JDE) without the approvals as per local DoA. The same users should not be allowed to make adjustment in the production tools (e.g TIS for cement sites) and ERP (e.g SAP, JDE) inventory modules.
- Discrepancies are analyzed to identify their sources and implement corrective and preventive actions. Any discrepancy over 5% for semi-finished and finished goods need to be investigated and documented with justifications.
- **Dead stock.** For all products, the total stock taken into account in the production data report includes the live stock (movable automatically with permanent equipment) and the dead stock (non movable automatically). The value of the dead stock is agreed upon between the production manager and the financial controller.
- **Zero & Full stock.** For bulk products, it is recommended to reach at least once a year a physical zero stock level in order to perform a consistency check between theoretical stock and physical stock. When a full-stock or zero-stock level is reached, discrepancy between book & physical stock must be adjusted.

Link to: HARP: Finance Policy, 3.1.1.1.6 Inventories, 3.2.1.2.30 Inventory Movements Finished Products

35 Inventory valuation

PRIMARY OBJECTIVE

Record the proper value of inventory by identifying and providing provision for obsolete or slow-moving items.

RISK
- Inaccurate or fraudulent recording and tracking of inventory (Step 1, 2)
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2)

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Approval of inventory costing and valuation according to local Delegation of authority (DoA).** ***Quarterly***
2. **Half yearly, for hard close events, approval by CFO (or designee) of provisions for obsolescence and slow moving parts and write-offs according to HARP.** ***Half year***

REQUIREMENTS

- The valuation of each type of inventory is reviewed for consistency with Group Accounting rules. Inventory costs include purchasing costs, conversion costs and other costs incurred in bringing the inventories to their present location and condition (excluding storage costs). (Step 1)
- Purchased products are valued at purchase price less any price deductions such as trade discounts and rebates. Expenses directly related to the acquisition (insurance, import duties, transport and handling costs etc.) are included in the value of the inventory. (Step 1)
- Inventory of own produced finished and intermediate products are valued based on actual cost of goods produced including depreciation and certain distribution costs (transport to terminals, warehousing, bagging, etc.). Standard costing can be used during the year. At year-end, inventories must be restated to actual cost. Standard cost should be updated at a minimum once per year at Year End (or Hard Close November). (Step 1)
- Inventory provisions (obsolescence and slow moving spare parts) and write-offs are estimated according to Holcim Accounting and Reporting Principles (HARP), based on appropriate supporting documents and applied consistently from one year to another. They are approved according to the delegation of authority. (Step 2)
- Review for obsolescence for slow moving parts and related provisions and write-offs are performed half yearly during hard close events. (Step 2)

Link to: Group Delegated Authorities (GDA), Finance Policy, Accounting for value adjustment for different types of inventory, HARP 3.1.1.1.6 Inventories

IT

36 Management of access to IT systems

PRIMARY OBJECTIVE

Management of access to IT systems is in place to prevent unauthorized access, disclosure, modification, damage or loss of data.

RISK
- Unauthorized access, disclosure, modification, damage or loss of data (Step 1, 2)

IMPACT
- Operational disruption
- Fraud

CONTROL & FREQUENCY

1. **Access to the IT systems will only be granted, changed or terminated based upon a correctly authorized access request as per defined procedure.** ***Upon Request***
2. **In the case of terminations, upon receipt of notification from HR/ business, IT to terminate all user access in a timely manner (3 working days for a power user, such as an administrator role, and 5 working days for a regular user).** ***Upon Request***

REQUIREMENTS

Note: Information Technology (IT) Systems refers collectively to Business Applications and IT Infrastructure (Operating System, Database, Network, interfaces)

Granting/Changing Access (Step 1):

- A formal user access request form should be filled out for every new or change request to Holcim information systems and the corresponding approver has to approve it ensuring compliance with segregation of duties (SoD) rules.
- Human Resources should confirm the identity of all internal users and the Holcim sponsor for external users.
- External User IDs and temporary Holcim employees must have a defined expiration date up to 12 months for these IDs (renewable). Based on the type of ID and associated risks the sponsor may choose to further limit this expiry to a shorter period (e.g. three months). Expiration may be set up at Google / Active Directory level where not supported by the application.

Termination (Step 2):

- The scope of this controls starts from the time Human Resources or Business notifies IT a request for termination of user. The control for business notification to IT is under MCS25. IT to revoke access within defined timeline upon Human Resources / business notification.

Link to: Information Technology Policy, Information Systems User Directive, Annex 09 IT Controls

37 Review of IT user access rights to production IT systems

PRIMARY OBJECTIVE

IT users have appropriate access as per their job role and authorization.

RISK
- Unauthorized access, disclosure, modification, damage or loss of data (Step 1, 2, 3)

IMPACT
- Operational disruption
- Fraud

CONTROL & FREQUENCY

1. **IT performs a half yearly review of all IT user access rights and permissions for accounts within the production systems. *Half year***
2. **Actions are proposed (lock, disable, remove user accounts) if access rights are inappropriate. Access changes performed are documented and appropriately retained. *Upon Request***
3. **Dormant account reviews are performed periodically for all IT users (e.g. user not logged-in for 30/60/90 days) and actions taken. *Half year***

REQUIREMENTS

Note: Information Technology (IT) Systems refers collectively to Business Applications and IT Infrastructure (Operating System, Database, Network, interfaces)

- This control must cover the review of all Information Technology (IT) function users (e.g. OS, DB & Network administrators, AD administrators, application support team from IT and all other IT users who have access to production IT systems). Access review of Business users access to IT systems is covered under MCS12 and therefore not in the scope of this control (Step 1, 2 and 3)
- An IT user cannot review their own access. The review confirms that access is in line with the IT users role and responsibilities. (Step 1)

Link to: Information Technology Policy, Information Systems User Directive, Annex 09 IT Controls

38 Security configuration settings and batch job management

PRIMARY OBJECTIVE

Security configuration settings are reviewed to provide reasonable technical assurance to prevent any unauthorized access to IT systems. Batch jobs are monitored to ensure data integrity

RISK

- Successful cyber attack (IT/OT) (Step 1)
- Data leakage of sensitive information (incl. non compliance with GDPR) (Step 1)
- Unauthorized access, disclosure, modification, damage or loss of data (Step 2, 3)

IMPACT

- Operational disruption
- Fraud

CONTROL & FREQUENCY

1. **Once a year, the security configuration settings of IT systems are reviewed to verify whether the settings are appropriate and enforced according to the defined security requirements for applications, Operating Systems and Database. Access to identified critical transactions is restricted to users as needed. *Annual***
2. **Access to batch job scheduling is appropriately restricted to authorized users and reviewed half yearly. *Half year***
3. **Every month the batch jobs and interfaces are monitored and processing errors are timely corrected. *Monthly***

REQUIREMENTS

Note: Information Technology (IT) Systems refers collectively to Business Applications and IT Infrastructure (Operating System, Database, Network, interfaces)

- Minimum Security Baseline requirements are defined in - Annex 09.01 Holcim Minimum Baseline Security Standard approved by the Group IT Security responsible. (Step 1)
- ITSC Security officer is responsible to obtain the IT system configuration settings and review them to ensure they are as defined (or stricter) in the Security configuration Baseline.(Step 1)
- For IT systems not managed by Holcim (e.g. Cloud hosted and managed by third parties) Business or IT should obtain independent audit report (e.g. ISAE 3402) from the service provider at least annually to verify and follow up on any IT internal control deficiency reported. (Step 1)
- Critical batch jobs (different from end user scheduled background jobs) are identified (e.g. interfaces between Enterprise Resource Planning (ERP) and other critical systems to ensure failures, if any are timely corrected to ensure data integrity). Access to such scheduled jobs is restricted. (Step 2, 3)

Link to: Information Technology Policy, Information Systems User Directive, Annex 09 IT Controls

39 Data backup, storage and restoration process

PRIMARY OBJECTIVE

Data backup, storage and restoration process is implemented to minimize loss of data

RISK
- Business disruption due to IT/OT unavailability (Step 1, 2, 3)

IMPACT
- Operational disruption
- Financial loss

CONTROL & FREQUENCY

1. **Backup is performed as per the schedule (daily, weekly, monthly etc.). Backup logs are monitored routinely to verify success / completeness. Errors, if any, are reported as incidents and resolved.** ***Daily***
2. **When external media is used, backup is stored offsite and media labeling procedures are defined and followed. When online data replication (e.g. SAN) is setup, data is protected against corruption (ensuring that corrupted production data may not be synced in realtime to the backup).** ***Upon Request***
3. **Restoration tests are performed at least annually. Failures, if any, are investigated and resolved.** ***Annual***

REQUIREMENTS

The IS_S04 IT Infrastructure and Operations Standard defines the IT Backup requirements. The local backup and restore procedures should document:

- Scheduling
- Backup rotation
- Retention times
- Testing of restoration process
- Evidence that backup are performed
- Evidence of tests performed regarding the restoration procedure

Backup strategy should be designed taking into consideration that risk of data loss and data corruption is minimized (e.g. controls to prevent backup data corruption). The restoration should be achievable within the business agreed recovery and restoration time objective. (Steps 1, 2, 3)

Link to: Information Technology Policy, Information Systems User Directive, Annex 09 IT Controls

40 Managing changes to IT systems

PRIMARY OBJECTIVE

Prevent unauthorized changes in IT systems.

RISK
- Unauthorized changes to the IT systems (Step 1, 2, 3, 4, 5, 6)

IMPACT
- Operational disruption
- Fraud

CONTROL & FREQUENCY

1. **There is verification that the requester is authorized to request changes to the relevant IT systems. *Upon Request***
2. **There is a verification that the requester has followed defined procedure for requesting changes and that the requests are approved as required. *Upon Request***
3. **User Acceptance Test is performed (there may be additional tests for the Unit and Integration Test, if required). Results of User Acceptance Test record who performed the User Acceptance Test and when. *Upon Request***
4. **There is a verification on the release authorization (ensures evidence of who authorized the release and when). *Upon Request***
5. **There is verification that segregation of duties is maintained especially that the developer does not move their own changes into the production environment. *Upon Request***
6. **There is a verification on the existence of test and log evidence to support the assertion of secure movement of changes into production (where changes are applied directly on production systems e.g. a configuration or security setting change, it is reviewed and confirmed for correctness). *Upon Request***

REQUIREMENTS

Note: Information Technology (IT) Systems refers collectively to Business Applications and IT Infrastructure (Operating System, Database, Network, interfaces)

- Changes to IT systems should be requested only by authorized approvers (application super users, business process owners) to ensure that only valid changes for business needs are requested (Step 1).
- To request changes a defined procedure is followed where the approvals are captured and recorded (Step 2).
- User Acceptance Test (UAT) should not be performed by the developer / change responsible to ensure segregation. User Acceptance Test is generally performed by the application super users or business / function approved testers (Step3).
- The change approval board (CAB) verifies all changes before providing release approval. Changes should not be moved to production without approval. (Step 4)
- Developers should not have change access to production system. The changes in production environment should be moved by administrators (BASIS for SAP ERP) (Step 5).
- Post change monitoring is performed to ensure there changes were correctly implemented (Step 6)

Link to: Information Technology Policy, Information Systems User Directive, Annex 09 IT Controls

Accounting & Consolidation

41 Compliance with accounting and reporting standards

PRIMARY OBJECTIVE

Implement and comply with all Holcim Accounting and Reporting Principles (HARP) accounting and reporting standards.

RISK
- Non-adherence to accounting and reporting requirements and standards (Step 1)

IMPACT
- Errors in financials

CONTROL & FREQUENCY

Confirmation by the CFO of compliance to HARP and IFRS through financial certification. Any deficiencies identified in a sustainability review conducted by the STAP team are remediated per the agreed timeline. *Annual*

REQUIREMENTS

- The Company's Chief Financial Officer is responsible for ensuring that Holcim Accounting and Reporting Principles (HARP) is sustained in the Company including updating the internal policies for the Holcim Accounting and Reporting Principles change releases. Adherence to Group standards is included in the annual certification letter.
- The Holcim Accounting and Reporting Principles and rules must be implemented in the Enterprise Resource Planning (ERP) systems (SAP, JDE, etc.) of all Holcim Group companies. This implementation is certified by the Group Standards and Accounting Principles (STAP) team who conducts a detailed review.
- Each Holcim Group company must have an appointed responsible for Holcim Accounting and Reporting Principles (HARPist). The CFO is responsible to appoint the HARPist, who is an integrated member of the HARPist Virtual Organization - an extension of the Standards and Accounting Principles (STAP) Team. HARPist must be recorded in the Company List.
- Regular Holcim Accounting and Reporting Principles (HARP) Compliance Reviews (cf. 7.4.4 HARP Sustainability Review) are conducted by the Standards and Accounting Principles team based on an annual plan.Any deficiencies identified must be monitored and remedied by the CFO (or designee).
- The Holcim Accounting and Reporting Principles Manual includes International Financial Reporting Standards (IFRS) elements that are relevant for Group reporting purposes. In the case where local circumstances dictate that a specific International Financial Reporting Standards, which is not documented in the HARP Manual, is applied, it is the responsibility of the Company's CFOs to ensure that the International Financial Reporting Standards is followed (in addition to HARP).

Link to: Finance Policy, HARP Manual, 7.4.4 HARP Sustainability Review

42 Reconciliation of general ledger accounts

PRIMARY OBJECTIVE

Reconcile and review balance sheet accounts and CFO sign-off of the trial balance and non-consolidated financial statements

RISK

- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2, 3)
- Non-adherence to accounting and reporting requirements and standards (Step 1, 2, 3)

IMPACT

- Errors in financials

CONTROL & FREQUENCY

1. **Communication and monitoring by the CFO (or designee) of a monthly closing checklist.** ***Monthly***
2. **Approval by the CFO (or designee) of income statements, balance sheet accounts, cash flow at least quarterly.** ***Quarterly***
3. **Approval by the designated financial person of subledger to general ledger (GL) reconciliations and trial balance monthly.** ***Monthly***

42 Reconciliation of general ledger accounts

REQUIREMENTS

- The CFO (or designee) prepares and communicates a closing checklist or other document of key activities that must be performed during a close, including who performs the task and the deadline, which is monitored. (Step 1)
- The CFO (or designee) performs an analytical review of the income statement, balance sheet and statement of cash flows to look for variances exceeding the locally defined thresholds (% and amount in local currency) in comparison to the prior year and to forecast or budget. All significant deviations are explained in writing and all errors are corrected prior to final closing. Significant deviations discovered in the review are disclosed in writing. Once completed, the CFO (or designee) approves the income statement, balance sheet and statement of cash flows in the Group Reporting Unit's reporting package. (Step 2)
- The system automatically posts subledger entries to the general ledger and blocks posting of manual entries directly to the general ledger. Any adjustments should be made directly to the subledger. (Step 3)
- The subledger is reconciled to the general ledger monthly to ensure the total balance per the subledger agrees with the total per the general ledger. Any differences are documented, investigated and cleared (all corrections made to the subledger). The reconciliation is approved by the designated finance person. (Step 3)
- For leases under the scope of International Financial Reporting Standards 16 (IFRS 16), lease payments must be reconciled between SAP Flexible Real Estate Management (RE-FX) and the local vendor accounting in the Enterprise Resource Planning (ERP) system. Right of use assets and the Lease Liability account should be reconciled with the sub-ledger (the detail by contract), by comparing fixed asset ledger and general ledger (GL). (Step 3)
- After all closing journal entries have been booked and the subledger to general ledger reconciliations have been finalized a trial balance, the listing of the general ledger balances by account on the last day of the month, is analyzed and reviewed. Possible errors in the trial balance, which are noticed as part of the review, are corrected before the final closing. Significant deviations are disclosed in writing. Once completed, the trial balance is approved by the designated finance person. (Step 3)

Link to: Finance Policy, Lease Directive

43 Reconciliation of bank accounts

PRIMARY OBJECTIVE

All bank accounts are reconciled to the general ledger regularly, signed by the CFO, and adjustments are recorded immediately.

RISK
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1)
- Non-adherence to accounting and reporting requirements and standards (Step 1)

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Monthly bank statements are obtained from the banks and reconciliations with the general ledger (GL) are performed by the finance responsible. Required adjusting entries are booked and all unreconciled items are followed up for closure within 90 days. The CFO (or designee) approves the monthly reconciliation.** ***Monthly***

REQUIREMENTS

- A proper segregation of duties (SoDs) is in place between reconciliation, booking and approval activity. The person who performs the bank reconciliations must not have access to recording of transactions in the accounting system or to process cash disbursements or receipts.
- At least monthly, all bank statements are reconciled to the general ledger account timely. The accounts denominated in foreign exchange rates (FOREX) are recalculated according to the month-end rate and the impact is recorded in the general ledger. The bank statement, the general ledger (GL) balance and the related journal entries are attached in the bank reconciliation. Reconciling items (identified differences between the book and bank balances) are followed up timely and are aged. Any adjustments required to the general ledger are recorded before closing. All bank reconciliations (even for inactive or dormant accounts) at each month-end closing are reviewed and approved by the CFO (or designee).
- Local banking regulation over clearance of bank transactions to be taken into consideration for quick identification of unreconciled items.
- All reconciling differences should be identified, explained and, when applicable, appropriate action for resolution formalized. Any necessary journal entries to resolve the differences should be posted no later than 90 days after the reconciliation is done. The bank should be contacted concerning any bank errors which should also be resolved within 90 days. The usage of suspense accounts are not allowed.

Link to: Finance Policy, Group Treasury Directive, HARP Manual 3.1.1.1.2 Cash and Cash Equivalents

44 Reconciliation of intercompany balances

PRIMARY OBJECTIVE

All intracompany and intercompany balances are reconciled with the partner to ensure accuracy of the general ledger and proper elimination upon consolidation.

RISK
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2, 3)
- Non-adherence to accounting and reporting requirements and standards (Step 1, 2, 3)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Signed contract documented and filed for all intercompany transactions.** ***Upon Request***
2. **Review and approval by the designated financial person of the intercompany and intracompany accounts each month, including a confirmation with each partner (or documentation that balances agree in Reco-Live).** ***Monthly***
3. **All applicable intercompany invoices are set to be settled through the netting platform within the defined agreed timing. (GRU's in scope).** ***Upon Change***

REQUIREMENTS

- Each intercompany transaction between different legal entities must have a signed contract. Each intercompany invoice must include relevant details for the goods or services provided based on a signed contract. (Step 1)
- All balance sheet and income statement intracompany and intercompany accounts are formally reconciled with each partner unit, including other companies of the Holcim Group. Reconciling items must be identified and corrected before the end of the close. Any FX difference (between the spot rate and the AV rate) on the cash flow with a Group partner needs to be communicated & documented to Corporate Reporting before the publication of the consolidated package.The reconciliations should be reviewed and approved by the designated finance person. This ensures that intercompany balances are fully eliminated in consolidation. (Step 2).

Standardized Intercompany Settlement Process

- The Group Reporting Unit (GRU's) CFO must prepare the integration plan and seek approval by the Head Group Treasury. (Step 3)
- Intercompany invoices (excluding loans, interest, dividends) must be settled through the netting platform (Coprocess) where both parties (payer/payee) are in scope (GRU in scope). (Step 3)

Link to: Finance Policy, Recharges to Corporate Directive, HARP: 7.3.3 Reconciliation Policy, 7.3.3.2 Reconciliation process, 4.11.2 Accounting Treatment for Invoicing of Services within Holcim – other than Industrial Franchise Fee (IFF) , 4.11.3 Accounting Treatment for Group Charges - Administrative Support Fee (ASF)

45 Manual journal entries

PRIMARY OBJECTIVE

Manual journal entries are properly supported, reviewed and approved by appropriate personnel.

RISK
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2, 3)
- Non-adherence to accounting and reporting requirements and standards (Step 1, 2, 3)

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Ensure that all manual journal entries are approved as per country Delegation of authority by the designated finance person, together with supporting documentation prior to posting.** ***Upon change***
2. **Quarterly verification and sign-off by the responsible manager to ensure only approved users from accounting function have access to post manual journal entries. Quarterly approval by the Countries of a list of approved persons who can request manual journal entries to the Business Service Centers.** ***Quarterly***
3. **Monthly verification and sign-off by the CFO (or designee) of the analytical review report.** ***Monthly***

REQUIREMENTS

Manual journal entries are considered high-risk transactions; therefore they must be kept to a minimum.

Scope: Manual Journal Entries (MJEs) are Journal Entries posted by a user/person and are not system triggered /automatic entries in the Enterprise Resource Planning (ERP) application (e.g. accounts payable (AP) or accounts receivable (AR) ledger posting). Manual Journal Entries are prepared by individuals to capture economic activities outside of sub-ledgers, i.e. directly in the general ledger. When Manual Journal Entries (MJEs) are used, proper process review and approval is in place as detailed below.

- Proper Segregation of Duties (SoD) lies between Manual Journal Entries requester, approver, and those posting the entries.(Step 1)
- Manual journal entries should be posted in the system after they are reviewed and approved. All Manual Journal Entries require approval before posting. Additionally, entries relating to valuation adjustments should be approved by the CFO. (Step 1)
- All manual journal entries are required to have adequate supporting information/ documentation, appropriate business rationale, recorded within the right period, with the right amount. If the entry is performed at a Service Center, these information/documentation have to be provided to them in order for the posting to take place. (Step 1)
- Only users in the accounting function are allowed to have access to post manual journal entries.(Step 2)
- The CFO (or designee) performs a monthly analytical review of manual journal entries posted (including all required reversals).This includes statistics on the number of entries, nature/type and amount of journal entries to detect any unusual activity as part of the review. Countries define locally the thresholds and unusual items for the review. The reviewer is a person other than someone who is posting the entries. (Step 3)

Link to: Finance Policy, Annex 14 SAP MJE's Regional scope

46 Impairment of goodwill, intangible assets and tangible assets

PRIMARY OBJECTIVE

Perform an impairment test for goodwill, intangible assets and tangible assets to ensure that their recorded values are not greater than their recoverable amount.

RISK

- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2, 3)
- Non-adherence to accounting and reporting requirements and standards (Step 1, 2, 3)

IMPACT

- Errors in financials

CONTROL & FREQUENCY

1. **Approval by the Group CFO of the goodwill impairment test template assumptions and Mid-Term Plan (MTP) cash flow data together with other additional data used for the estimate of value in use. (Group Level).** ***Annual***
2. **At least annually, approval by the Country CFO (or designee) of the impairment tests for other intangible assets with indefinite lives and tangible assets annually or if a triggering event occurs and, if an impairment exists, review of the impairment loss and possible adjustment to the carrying value and useful life (if applicable).** ***Annual***
3. **Notification of impairment issues by the country CFO (or designee) to the Group Corporate Reporting team by using the goodwill impairment template at all times as they occur and before the end of May and November.** ***Half year***

REQUIREMENTS

Cash Generating Unit (Step 1):

- As from January 1, 2019 a Cash-Generating Unit (CGU) for goodwill impairment testing from country or regional cluster level to operating segment level. This emphasizes the level of responsibility of regional Management with focus on segment performance. The Group's cash-generating units continue to be defined on the basis of the geographical markets, normally country- or region-related. For the purpose of Goodwill impairment testing, the Group's cash-generating units are aggregated into an operating segment, which is the level reviewed by the Group CEO (i.e. chief operating decision maker). The operating segments on which goodwill will be tested for impairment would be as follows:
  - North America; Europe; Middle East Africa; Latin America; Asia Pacific (excluding China) and China.

Goodwill: Guidance (Step 1)

- Consequently , all goodwill is tested for impairment by Corporate Reporting in Zug, Switzerland and not by a Group Reporting Unit. The Group goodwill impairment test template will be used to test for impairment. The cash flows contained in the Mid-Term Plan form the basis of the test with additional information required. The calculations and assumptions must be validated and approved by the Group CFO.

Other intangibles with indefinite lives (Step 2):

- At least annually or if a triggering event occurs, a test of impairment of an intangible asset with an indefinite useful life (or an intangible asset not yet available for use) is completed by comparing its carrying amount with its recoverable amount.

PPE (Property Plant & equipment) (Step 3):

- Group companies shall use the goodwill impairment template at all times when assessing Property, Plant and Equipment (PPE) for impairment.
- All designated assets are assessed at least annually to determine if there is any indication of impairment. If indicators are present, a formal estimate of the recoverable amount of the asset must be calculated. The review needs to be documented and must be formally approved by the appropriate finance person.
- If it is determined that there is an impairment, the impairment loss must be recognized immediately to the extent that the carrying value is greater than the recoverable amount.
- If there is an indication that an asset may be impaired, the remaining useful life of the asset should be reviewed and adjusted, if needed, even if no impairment loss is recognized.
- Group Corporate Reporting should be notified if any impairment issues arise before the end of May and November.

Sustainability (Step 3):

- An impairment might be required if a tangible asset becomes obsolete, is replaced earlier than expected, or cannot be used anymore as a result of newly introduced stringent environmental measures.

Link to: Group Delegated Authorities (GDA), Finance Policy, HARP 4.4.3 Impairment of Assets, Annual ARC impairment model and impairment testing guidelines

47 Transactions in a foreign currency

PRIMARY OBJECTIVE

Identify, record and revalue all transactions in a foreign currency and recognize foreign currency gains/losses.

RISK

- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2)
- Non-adherence to accounting and reporting requirements and standards (Step 2)
- Improper management of foreign exchange risk (Step 1)

IMPACT

- Errors in financials

CONTROL & FREQUENCY

1. **Approval by either IT Service Centers (ITSCs), CFO (or designee) that the correct Group communicated exchange rates were entered into the Enterprise Resource Planning (ERP) system daily or at least monthly.** ***Monthly***
2. **Analytical review of the foreign currency gain or loss in the general ledger to ensure all foreign currency transactions were properly revalued using the month end rate.** ***Monthly***

REQUIREMENTS

- Daily exchange rates published by central banks are usually used to record receivables and liabilities relating to the foreign currency transaction (settlements, recognized gains/losses). The exchange rate used in the Enterprise Resource Planning (ERP) system on the last day of the month is the official rate calculated and defined by the Group and communicated to all countries. Exception (i.e. utilization of daily rates from central bank for the last day of the month, instead of the rates communicated by the Group) must be approved by Group Corporate Reporting based on appropriate impact analysis performed on a bi-yearly basis. (Step 1)
- A foreign currency transaction is one that requires settlement, either payment or receipt, in a foreign currency. Such transactions are identified and recorded in the general ledger as a foreign currency transaction (denominated in the currency of the transaction so the Enterprise Resource Planning (ERP) system can automatically revalue the transaction until settlement). (Step 2)
- Where a transaction is not settled in the same reporting period as that in which it occurred, it must be revalued using the closing rate of the reporting currency. Any resulting gain or loss must be recognized in the income statement as a foreign currency gain or loss. If recorded in the system in the currency of the transaction (foreign currency), this will be done automatically by the Enterprise Resource Planning (ERP) system. If not, this must be done manually. (Step 2)

Link to: Finance Policy, Group Treasury Directive, Foreign Exchange (FX) & Interest Rate (IR) Risk Management Directive,HARP: 3.2.4.4 Foreign Exchange Losses (Gains), 4.7.1 Accounting for the Effects of Changes in Foreign Exchange Rates

48 Management of legal structure and consolidation hierarchy

PRIMARY OBJECTIVE

Ensure a complete and correct scope of consolidation by proper reporting and disclosure of the legal ownership rights.

RISK
- Non-adherence to accounting and reporting requirements and standards (Step 1, 2)
- Absence of control and supervision over remote or small entities (Step 1, 2)

IMPACT
- Errors in financials

CONTROL & FREQUENCY

1. **New legal entity and/or any changes in the structure of legal entity must be updated in the Umbrella tool within 3 days of incorporation or change. The Group Reporting Unit CEO and CFO verifies the legal entity structure and signs off the Legal Entity Management Tool (Umbrella) information half yearly according to Group Accounting, Reporting, Consolidation and Controlling (ARC)/ Group Legal Instructions (Hard Close May & Nov).** ***Half year***
2. **Approval by the designated finance person together with legal of the consolidation hierarchy percentage of ownership and any put/call liability to ensure correct accounting and reporting treatment (e.g. consolidation method) and reconciliation to the financial investments in the statutory accounts before the start of the country consolidation.** ***Monthly***

48 Management of legal structure and consolidation hierarchy

REQUIREMENTS

- The creation of any new legal entity must be in accordance with the Group Delegated Authorities. The Group Reporting Unit (GRU) CEO is responsible to ensure that all legal entities without any limitation of scope, materiality or percentage of participation with direct or indirect control are documented in the Legal Entity Management Tool (Umbrella). Sign off by the CEO and CFO confirming completeness and accuracy of reported information performed during the May and November hard close events. (Step 1)
- All information in Legal Entity Management Tool (Umbrella) is updated within 3 days after any change occurs. (Step 1)
- All information in Legal Entity Management Tool (Umbrella) is compulsory and must be completed accordingly. Legal documents must be uploaded in Umbrella as defined by the UMBRELLA USER GUIDE, section 11. (Step 1)
- Reconciliation over the agreed consolidation hierarchy, with Enterprise Resource Planning (ERP) system and Legal Entity Management Tool (Umbrella) to take place whenever a change occurs, or at least bi-yearly. (Step 1,2)
- On a monthly basis, before the start of the country consolidation, the consolidation hierarchy is reviewed by the local reporting team to verify the completeness and correctness of the Enterprise Resource Planning (ERP) system set-up of the legal entities, the consolidation methods and the legal ownership percentages. In case of changes and/or doubts, alignment with legal is required and the Group Consolidations team needs to be informed accordingly. If a transaction is considered to be a change in structure (CIS), then it must be documented (legal entity, % of ownership, parent, method of consolidation, etc.). If the transaction meets the threshold, it is recorded as a change in structure (CIS) movement in the SAP- Financial Consolidation (SAP-FC) package. (Step 2)

Link to: Group Delegated Authorities (GDA), Finance Policy, Group Treasury Directive, Legal Entity Management Tool (Umbrella) User Guide

49 Consolidation of financial statements

PRIMARY OBJECTIVE

Review of the reporting package, including equity and consolidation entries, and approval of the reporting package and supporting schedules before submission to the Group.

RISK
- Non-adherence to accounting and reporting requirements and standards (Step 1, 2)
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2)

IMPACT
- Errors in financials

CONTROL & FREQUENCY

1. **Review and approval by the CFO (or designee) of the reconciliation of local equity (general ledger) and local chart of accounts to the reporting package (SAP-FC).** ***Half Year***
2. **Review and sign-off by the CFO (or designee) of the SAP- Financial Consolidation (SAP-FC) reporting package before submission as per the requirements.** ***Monthly***

REQUIREMENTS

- A review is performed to ensure the amounts reported in the group reporting package in SAP- Financial Consolidation (SAP-FC) are correct and complete. The mapping between the local chart of accounts and the consolidation package, if applicable, is formalized and any change is authorized by the designated finance person. (Step 1)
- When a country performs a sub-consolidation, the consolidated reporting package is reviewed for the completeness and correctness of the consolidation, where applicable, including (Step 1):
  - Eliminations, taking into consideration any non-controlling interest calculation
  - Accounting for any deconsolidation, acquisition, merger or transfer.
  - Conversion to the reporting currency and related currency translation adjustment are reviewed for reasonableness using the rates published by the Group (and used in SAP- Financial Consolidation).
- A reconciliation of local equity (general ledger) to the Group consolidation accounts (SAP- Financial Consolidation) is performed twice a year (mid year and year end), approved by the CFO (or designee) and uploaded in Umbrella. Differences are explained, documented and recorded. (Step 1)
- The country reporting package is reviewed and approved by the appropriate finance person country CFO (or designee) before being submitted to the Group. The CFO (or designee) formally signs off on the financial statements to confirm that they have been reviewed, that the amounts reported are correct and that all relevant information for disclosure purposes has been included in the appendices. (Step 2)

Link to: Finance Policy, ARC Permanent Instructions 2023, Umbrella User Guide

50 Statutory financial statements

PRIMARY OBJECTIVE

Statutory financial statements are reconciled to Group financial statements, reviewed and signed off by the CFO and statutory audits are completed by April 30th.

RISK
- Non-adherence to accounting and reporting requirements and standards (Step 1, 2, 3)
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2)

IMPACT
- Errors in financials

CONTROL & FREQUENCY

1. **Review and sign-off by the CFO (or designee) on 1) the reconciliation between the Group reporting package and the statutory financial statements and all adjustments made, 2) the statutory financial statements, including related disclosures and 3) the reconciliation between the Group reporting package and the statutory financial statements is uploaded in Umbrella.** ***Annual***
2. **Audit qualifications on the local financial statements, if any, must be reported to the Group ARC together with the signed statutory audit reports of a calendar year by April 30th of the following year. Any exceptions must be approved by the Head of Group ARC before the April 30th deadline.** ***Annual***
3. **All listed companies must receive formal approval by the Head of ARC and Group CFO before any external publication of press releases including statutory accounts.** ***Upon Change***

REQUIREMENTS

- Audit fees negotiation and all additional audit related fees for all Group Companies and change of auditor at country level approvals according to Group Delegated Authorities (GDA) and Approval of audit, audit-related and non-audit services Directive.
- A reconciliation between the financial statements per the Group reporting package and the statutory financial statements must be performed to ensure amounts are correct and complete. (Step 1)
- A reconciliation by flow of the equity between the Group reporting package and the statutory financial statements must be provided in Umbrella once the statutory financial statements are signed by the auditors based on a comprehensive template. (Step 1)
- Any adjustments made to the SAP-Financial Consolidation (SAP-FC) financial reporting package (financial statements) to comply with the regulations of the statutory financial statements (e.g. International Financial Reporting Standards (IFRS) to a local Generally Accepted Accounting Principles (GAAP) must be documented and approved by the CFO (or designee). (Step 1)
- The CFO (or designee) formally signs off on the statutory financial statements to confirm that they have been reviewed and the amounts reported, including all relevant disclosures, are correct. (Step 1)
- All statutory audits of a calendar year must be completed by April 30 of the following year. Any exceptions must be approved by the Head of Group Accounting, Reporting, Consolidation and Controlling (ARC). Exceptions must be granted before the April 30th deadline, otherwise the MCS is not adequate. The CFO (or designee) ensures that root cause of delays are analyzed and the organization and process is improved for the next year. (Step 2)
- For both the statutory and group audits, a mandatory audit firm rotation is to take place every 10 years the latest (more frequent intervals may be applied by the management). A previously appointed audit firm, after its rotation, cannot be re-elected for a period of at least 3 years. Additionally, key audit partners must rotate every 7 years the latest. A previously appointed key audit partner, after his/her rotation, cannot be re-elected, irrespectively of the audit firm in which he / she might work for. If local regulations of each country of incorporation, dictate a more frequent mandatory rotation of audit firms or key audit partners and / or a longer waiting period for re-election, then local regulations supersede this guidance and the more frequent rotation periods and/ or the longer waiting periods should be applied locally. Refer to the Directive of approval of audit, audit-related and non-audit services. (Step 2)
- All listed companies, at least 7 days before the release of the statutory accounts, must (1) Provide a reconciliation of the equity as well as the main indicators of the P&L to the Head of ARC and the Region CFO. This must be reviewed and confirmed by the Head of ARC and the Region CFO (2) Obtain formal approval by Head of ARC and Group CFO before any external publication of press releases including financial reporting. (Step 3)

Link to: Group Delegated Authorities (GDA), Finance Policy, Approval of audit, audit-related and non-audit services Directive, ARC permanent instructions 2023, Umbrella User Guide

Tax

51 Tax risk assessment and reporting

PRIMARY OBJECTIVE

Track, monitor and reduce tax risks and ensure they are properly reflected in financial statements and disclosures.

RISK
- Lack of proper tax risk monitoring and reporting (Step 1, 2)
- Poor management of tax cases (Step 1, 2)
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1, 2)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Quarterly review and approval by the country CFO (or designee) of the provisions reported and the full list of uncertain tax position as per the requirement, at the Country/ Group Reporting Unit level, and confirmation they agree to the amounts in the financial statements.** ***Quarterly***
2. **Review and approval of tax risks, at the consolidated Group level, by the Group Head of Tax every quarter to ensure all required information is reported, complete and updated with the latest assumptions. (Group level)** ***Quarterly***

REQUIREMENTS

At least quarterly, the country CFO (or designee) keeps track of and reviews the status of all uncertain tax positions, including (Step 1):

- The estimated maximum risk and estimated loss,
- The classification as not probable, probable and virtually certain,
- The amount of the provisions recorded in the financial statements.

Based on this information:

- Provisions must be adjusted accordingly
- Contingencies must be disclosed

This detailed information is reported to Group Tax using the format and tool communicated by Group tax with all balances reconciled to SAP - Financial Consolidation (SAP-FC). (Step 2)

Link to: Group Delegated Authorities (GDA), Finance Policy, Tax Reporting Directive, HARP 7.3.4.04 Tax Risk Reporting

52 Tax filings and payments

PRIMARY OBJECTIVE

Any exceptions to timely tax filings and payments must be approved by the Group Head of Tax.

RISK
- Statutory filings and payments not performed timely (Step 1, 2, 3)
- Poor management of tax cases (Step 1, 2)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Local tax responsible and CFO (or designee) to implement a tax calendar with all tax filing and payment due dates.** ***Annual***
2. **Approval of the calendar by the local tax responsible to ensure that all filings and payment are made on time.If an extension is needed, the local tax responsible obtains approval from the Group Head of Tax.** ***Annual***
3. **Identification and timely disclosure of reportable cross border transactions as per local requirements.** ***Upon request***

REQUIREMENTS

- A tax calendar, including filing and payment due dates for all taxes, is formally set up by the local tax responsible and CFO (or designee). (Step 1)
- A process is in place to monitor filings and payments so they are made on time. Entities should be compliant with local rules for timely filing and payment of tax liabilities. Any extension request for filing or payment of taxes shall be approved by Group Head of Tax. (Step 2)
- Following local rules, the identification and timely disclosure of reportable cross border transactions to tax authorities, when/where applicable. (Step 3)

Link to: Group Delegated Authorities (GDA), Finance Policy, Tax Reporting Directive, European Mandatory Disclosure Regime Directive

53 Deferred and current income tax calculations

PRIMARY OBJECTIVE

The deferred and income tax calculations and related documentation are prepared in accordance with the Group consolidation instructions, tax policies, directives and guidance and in line with local tax regulations.

RISK
- Inaccurate or fraudulent closing entries (incl. judgmental assumptions and estimates) (Step 1)
- Lack of proper tax risk monitoring and reporting (Step 1)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Review by the local tax responsible and approval by the CFO (or designee) of all income tax and deferred tax calculations and related documentation at least quarterly.** ***Quarterly***

REQUIREMENTS

A quarterly review of the deferred and current income tax calculations and related documentation is performed by the local tax responsible and CFO (or designee) and includes:

- Appropriate representation on outstanding audits
- Compliance with requirements of tax rulings
- Enacted tax rate changes
- Tax Risks Provisions/Uncertain Tax Positions (UTPs) and exposures including analysis of changes and or expirations, quantification, and probability assessment
- Documented analysis of any temporary differences between the tax basis of an asset or a liability and its carrying amount per the Statement of Financial Position and proofs of all deferred tax balances
- Reconciliation with amounts booked in the consolidation package
- Tax rate reconciliation (prepared, documented, and validated)
- Recoverability of deferred tax assets is justified by supporting evidence
- Account reconciliation ending balances are verified to ensure all accounts requiring reconciliation are identified and ending balances on the reconciliations are correct.

Link to: Group Delegated Authorities (GDA), Finance Policy, Tax Reporting Directive, HARP: 3.1.1.2.7 Deferred Tax Assets, 3.1.2.2.3 Deferred Income Taxes, 3.2.6 Income Taxes.

54 Transfer pricing

PRIMARY OBJECTIVE

All tax and legal rules regarding intercompany transfer prices and documentation are complied with; transfer prices are entered in the relevant systems; where required, transactions are reviewed by Group Tax. Any exceptions are discussed and approved by the Group Head of Tax

RISK
- Lack of commercial strategy and pricing policy (Step 1, 2)
- Lack of proper tax risk monitoring and reporting (Step 2, 3, 4)
- Poor management of tax cases (Step 1, 2, 3, 4)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Determination and confirmation by Group Tax and Regional Heads of Tax on the methodology used for intercompany transactions. (Regional & Group level)** ***Annual***
2. **Agreement by the Group Head of Tax on any exception to the Holcim Direct Taxation policy. (Group level)** ***Annual***
3. **Review and analysis by the local tax responsible and approval by the CFO (or designee) to check that the practice of the entity is in compliance with the Group Transfer Pricing Directive.** ***Annual***
4. **Maintenance by the local tax responsible of transfer pricing documentation in accordance with local requirements.** ***Annual***

REQUIREMENTS

- Group Tax and the Regional Heads of Tax are analyzing, advising and confirming the transfer pricing methodology for all intercompany transactions. Transfer prices are entered into the relevant systems in order to ensure compliance with the Group Transfer Pricing Directive. (Step 1)
- Any and all intercompany transactions must comply with the arm's-length principle as also required by local laws and regulation. (Step 1)
- Any exceptions to the Group Transfer Pricing Directive for goods sold and services / intellectual property licenses within the Group (including rebates and one offs) should be discussed with Group Tax to evaluate the risk and has to be formally agreed by the Group Head of Tax (Step 2)
- The practice of the entity is regularly analyzed by the local tax responsible and the CFO (or designee) to check compliance with the Group Transfer Pricing Directive. Risk analysis is communicated to the finance and legal departments to define potential needs for provisions or disclosures in accordance with the Minimum Control Standards (MCS) on Tax Risks. (Step 3)
- Transfer Pricing Documentation is drafted, maintained and filed by the local tax responsible with the support of the Group Head of Transfer Pricing in accordance to local tax regulations and requirements. (Step 4)

Link to: Group Delegated Authorities (GDA), Finance Policy, Trading Policy, Direct Tax Directive, Transfer Pricing Directive (Intercompany overland transfers of clinker,cement, cementitious in Europe), Intellectual Property Directive

55 Non-income (indirect) taxes

PRIMARY OBJECTIVE

Non-income tax returns and related account reconciliations are prepared, reviewed and approved in line with the locally required frequency and local tax requirements.

RISK
- Statutory filings and payments not performed timely (Step 1, 2, 3, 4)
- Lack of proper tax risk monitoring and reporting (Step 2)
- Poor management of tax cases (Step 2)

IMPACT
- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Review and approval of all Value Added Tax (VAT) and indirect tax returns by the CFO (or designee).** ***Upon request***
2. **Review and approval by the local tax responsible of the reconciliation of current month activity per the tax calculation with the amount in the financial statements.** ***Monthly***
3. **Review by accounting responsible and approval by the local tax responsible of reconciliations of all Value Added Tax (VAT) accrual and recoverable accounts monthly.** ***Monthly***
4. **Review and approval by the local tax responsible of unusual activity in the Value Added Tax (VAT) reconciliations including Value Added Tax (VAT) litigations in progress.** ***Monthly***

REQUIREMENTS

- Value Added Tax (VAT) and indirect tax returns are prepared, reviewed and approved in line with local required frequency and local tax requirements. (Step 1)
- The reconciliation (base revenue, sales, others used to calculate Value Added Tax (VAT) or sales taxes with the recorded revenue, sales, others in Profit/Loss) summarizes current month sales activity to produce the monthly accrual needed. Any reconciling items noted during the reconciliation will be evaluated to determine a potential impact on the tax return. The reconciliation summarizes information based on current monthly accruals, quarterly accruals or annual accruals, based on the jurisdiction. Miscellaneous issues (missed payments, audit issues, etc.) are also noted and tracked on the reconciliation. (Step 2)
- The reconciliations for various Value Added Tax (VAT) accrual and Value Added Tax (VAT) recoverable accounts are performed by local accounting responsible. The local accounting responsible contacts the local tax responsible if they notice any unusual payments during the reconciliation process. (Step 3)
- Value Added Tax (VAT) payments are made from multipurpose cash accounts. The reconciliations for the cash accounts used to make Value Added Tax (VAT) payments are performed by the local accounting responsible as part of their cash account reconciliation process. Any unusual Value Added Tax (VAT) payments during the reconciliation process shall be reported to the local tax responsible. (Step 4)

Link to: Finance Policy

Treasury

56 Bank relations

PRIMARY OBJECTIVE

Bank relationship management – including all openings bank accounts – are managed and approved by Group Treasury in compliance with Treasury Directive requirements. All signatory guidelines in the Holcim Treasury Directive must be in place

RISK
- Unauthorized commitment or relationship with bank (Step 1, 2, 3, 4, 5)
- Transaction with sanctioned parties (Step 2)

IMPACT
- Compliance
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Obtain Group Treasury approval for any bank accounts that are opened and notification of closing bank accounts to Group Treasury.** ***Upon Request***
2. **Obtain Group Treasury approval for transaction with any counterparty not in the "Bank List" prior to initiating transactions within approved limits. Monitoring of the credit exposure within the concentration limit published by Group Treasury.** ***Upon Request***
3. **Annual approval of a list of all bank accounts and optimization plan by local CFO (or designee) based on Treasury directive including inactive bank account analysis and timely closing when applicable.** ***Annual***
4. **Quarterly verification by the local CFO (or designee) of the list of all open bank accounts reconciled with Legal Entity Management Tool (Umbrella) and local Treasury/ accounting system. At least, yearly confirmation of authorized signatories obtained from banks to ensure it is consistent with the delegation of authority (DoA).** ***Quarterly***
5. **Identified counterparty risk exposure breaches must be reported to the Head Group Treasury and corrective actions implemented within the agreed time frame.** ***Upon Change***

REQUIREMENTS

- Bank relations, including fees, approved as per Group Delegated Authorities (GDA), when applicable, and Group Treasury Directive. (Step 1,2)
- Any opening of bank accounts shall be approved by Group Treasury i/o Corporate Finance and Treasury (CFT). Any closing shall be notified to Group Treasury and updated in Legal Entity Management Tool (Umbrella). (Step 1)
- Information to the banks, including legal and compliance-related questions, needs to be provided in compliance with Group Treasury Directive. (Step 1)
- In order to limit credit exposure and concentration on any counterparty, the Group will only do business with authorized counterparties within concentration limits and guidelines described on the official Holcim Bank List. Within the Bank List, Relationship Banks should be considered over Niche Banks, unless Niche Banks offer a clear advantage.(Step 2)
- Business relationships with a bank not listed on the Bank List are subject to written approval by the Head of Group Treasury. Any counterparty risk with non-relationship or non-niche banks must be under the limit defined through the approval process by Group Treasury. Request for approval (RfA) procedure and form includes sanctions screening as per the Group Treasury Directive.(Step 2)
- The country CFO (or designee) reviews yearly the list of active and inactive bank accounts and ensures that the number of banks and bank accounts is optimized to increase visibility on cash and reduce risks and costs. If it is not optimized, a plan is set up for closing accounts by a specific deadline. (Step 3)
- Local reconciliation over approved bank accounts list with Enterprise Resource Planning (ERP) system and Legal Entity Management Tool (Umbrella) to take place whenever a change occurs, or at least quarterly. Ensure Legal Entity Management Tool (Umbrella) is up-to-date. (Step 3, 4)
- A process is in place to: (Step 4)
  - Ensure only joint signatory rights are allowed for any transaction with a bank and each signatory has sufficient seniority to become an authorized signatory. Implement authorization limits for individual roles appropriate to the size of the organization.
  - Ensure immediate removal of signatory rights for employees no longer involved in the payment process and inform the bank immediately in case of signatory changes.
  - Obtain from the banks the list of authorized signatures to confirm it is up to date and consistent with delegation of authority (at least once a year)
- Cash and deposit limit must be monitored. Any counterparty limit breach with non-relationship or non-niche banks shall be immediately reported with appropriate corrective actions to the Head Group Treasury. Corrective actions are implemented within the time frame agreed with group Treasury. (Step 5)

Link to: Group Delegated Authorities (GDA), Finance Policy, Group Treasury Directive, Sanctions and Export Controls Directive, Counterparty Risk Management: Concentration limit applicable to countries (Sept/21), Holcim Bank List 2021-2022 (Sept/21), Umbrella User Guide

57 Cash transactions are not permitted without Group CFO approval

PRIMARY OBJECTIVE

Cash transactions are not permitted without exceptional approval by Group CFO

RISK
- Unsecured payment means & cash transactions (Step 1, 2)
- Corruption and bribery (Step 1)
- Transaction with sanctioned parties (Step 1)
- Money laundering (Step 1)

IMPACT
- Compliance
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **If applicable, obtain Group CFO approval for cash transactions. Set up by the CFO (or designee) a local procedure with an approval process in line with the Holcim Group defined rules, controls and thresholds to safeguard and minimize cash and check transactions.** ***Upon Request***
2. **Monthly review and approval by the CFO (or designee) of the reconciliation of the checking and petty cash accounts.** ***Monthly***

REQUIREMENTS

Cash transactions can create opportunities for fraud, money laundering and the funding of bribes. For this reason, the general rule is that cash transactions are not permitted. If Group CFO approval is not formally granted, cash transactions are to be ceased. The following rules applies: (Step 1, 2)

- Maximum petty cash limit per site allowed is CHF 500. A petty cash is a small amount of cash kept on site to pay for minor expenses, such as office supplies or reimbursements
- Supplier payments in cash are not allowed.
- No cash collections are accepted from customers.
- Usage of checks is strongly discouraged and should be avoided. If used, only crossed checks are accepted (to be deposited to a bank account) for either supplier payment or customer receipt.
- Cash transactions to buy or sell foreign currencies at Exchange offices (Bureau de change) beside banks are strictly prohibited. Countries which need to conduct such transactions must get approval from the Group Head of Treasury.
- Holcim countries which have been granted Group CFO approval for cash transactions must perform restricted party screening on the third party (customer/supplier) in line with the Sanctions and Export Control Guidance.

Validate with Region Head of Finance and obtain Group CFO approval for any exception to the requirements listed above. If exceptions are approved, countries must implement a local procedure to: (Step 1, 2)

- Safeguard the process to issue and collect cash
- Track, record and support with appropriate documentation all approved cash and check transactions.
- Maintain segregation of duties between the person responsible for physical custody of cash/ checkbook and the bank and cash disbursement authorized signatories. Restrict access to check books/cash and to the safe to only designated persons so as to ensure segregation of duties.
- An independent person who is not responsible for the physical custody of checks shall physically verify unused checks on hand and reconcile with the checkbook register on a quarterly basis. Random inventory counting has to be performed several times a year by an independent person.
- Perform regularly (at least monthly) a reconciliation of checks and petty cash to the books. Investigate any variances, within the same period and confirm they are approved by the appropriate person before booking.

Link to: Finance Policy, Group Treasury Directive, Sanctions and Export Controls Directive (Sanctions and Export Controls Resource Center)

58 Secure payment means

PRIMARY OBJECTIVE

Payments are secured to avoid errors and safeguard assets.

RISK
- Unsecured payment means & cash transactions (Step 1, 2, 3, 4, 5, 6)
- Unauthorized access, disclosure, modification, damage or loss of data (Step 1, 2, 3, 4, 5)

IMPACT
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **All users with access to SAP-BCM and/or bank portals are approved by the CFO (or designee) as per the local DoA requiring dual approval for payments. In case of Business Service Centre users, the BSC Head approval is required.** ***Upon Request***
2. **Quarterly review of critical users with payment authorization, payment proposal upload, and administrator access by the CFO (or designee) for the country users or BSC Head (or designee) for the BSC users. Access is revoked within 3 business days for any inadequacy identified from the access review or for dormant users over 90 days with no valid justification.** ***Quarterly***
3. **Yearly review of non-critical users, view only access to bank balances, bank statements or bank monitor, by the CFO (or designee) for the country users or BSC Head (or designee) for the BSC users. Access is revoked within one (1) month for any inadequacy identified from the access review or for dormant users over 90 days with no valid justification.** ***Yearly***
4. **Changes to Business Partners master data are performed by an authorized user and based on an approved request. Upon Request**
5. **Quarterly verification and sign-off by the CFO (or designee) to ensure only users from dedicated functions (with no conflicting roles) have access to change Business Partner data.** ***Quarterly***
6. **At a minimum, annual validation by the Treasurer (or designee) of all active direct debits with the relevant counterparties (banks). Any direct debit not required is notified to the banks for cancellation.** ***Annual***

REQUIREMENTS

For bank transfers:

An inventory of all banks should be maintained with a list of users with bank portal and or SAP Bank Communication Manager (SAP-BCM) access (managed by country or Business Service Center) to ensure controls are applied. Access to any bank system including but not limited to SAP Bank Communication Manager and bank portal is strictly controlled.

- Each user has a unique ID and password, user access, for accessing the bank portals or SAP Bank Communication Manager. (Step 1)
- At least two authorized signatories approve bank payments (Step 1)
- No modification of data (payment files generated from a system) is possible along the whole process (e.g. supplier bank data, amount to be paid, payroll file etc.). Electronic transfers are coded/ encrypted by the system for security. Manual upload of payment files in banking platforms is not allowed. (Step 1)
- Banks systematically send a confirmation ensuring that the electronic file was received without communication errors (a negative or positive check or the possibility to verify) (Step 1)
- To minimize fraud risks, treasurers on a daily basis reconcile bank and intercompany accounts and refrain from communicating any details regarding the payment process to external parties other than banks (Step 1)
- Manual transfers (i.e. email requests or paper based such as letter or fax) must be strictly limited and the bank must call back the treasurer (or designee) (different from the one issuing the payment) once the manual transfer is received (to reconfirm before payment execution). Emails should be marked as confidential and attachments are password protected. Passwords must be communicated in a separate email (Step 1)
- Critical users: Quarterly, a list of all electronic banking users is obtained from the bank portal or banks. Users with payment approval access to SAP BCM transaction is obtained for review of SAP BCM access. Banks Payment authorization access is restricted to treasury operations / cash and banking teams. The review of users access to SAP BCM and bank portals is performed according to the users job role to ensure there is no unauthorized or conflicting access. Users with access to other processes in Enterprise Resource Planning (ERP) system (Master Data Management - MDM / Order to Cash - O2C / Procure to Pay - P2P / Hire to Retire - H2R) cannot have access on the bank portal or SAP BCM for payment approval. Reviewer should not review their own access. (Step 2)
- Non-critical users: Yearly, for users with view only access to bank balances, bank statements or bank monitor, a list of all users is obtained from the bank portal or banks and a review is performed to ensure only authorized users have the display access according to the user job role. Reviewer should not review their own access. (Step 3)
- Dormant users over 90 days should be reviewed. Users who no longer need access must be revoked in 3 business days for critical users and one month for non critical users and for others a justification / explanation should be documented as part of the review. (Step 2, 3)

58 Secure payment means

REQUIREMENTS

Business Partner master data (Step 4, 5)

- Entities that use Treasury management applications or any other payment platforms, where banks are setup as master data (referred to as Business Partners), a master data management process that defines roles, responsibilities and rules for Business Partner data management is in place and reviewed when required to ensure only authorized personnel create, modify and delete financially relevant Business Partner data based on the required supporting documents (SSI, RIB, IBAN ,...) and bank confirmation when required. Changes to bank information in the treasury applications or any other payment platforms must only be done post execution of the Call Back Process using the registered contact information on file. The call must be documented with a post confirmation via email.

Direct Debit (DD) (Step 6):

- Usage for vendor payment with direct debit is not permitted unless it is a mandatory requirement by the authorities (i.e. tax related payments). Any exception to the rule has to be approved by the local CFO and must follow all rules defined in the Group Treasury Directive.
- Treasurer (or designee) will ensure such direct debit payments are executed based on the agreements approved by the CFO.
- Inventory of the direct debit contracts signed has to be available for Treasury whenever applicable. Treasurer (or designee) will ensure regular confirmation (on a yearly basis minimum) of the inventory with the relevant counterparties (banks)

Link to: Finance Policy, Group Treasury Directive

59 Financial instruments, borrowings, commitments and working capital schemes

PRIMARY OBJECTIVE

All financial instruments, borrowings, commitments and working capital schemes are authorized in accordance with the Group Treasury Directive. Outstanding positions are reconciled with counterparty statements

RISK
- Inability to maintain an adequate cash flow and liquidity position to pay obligations (Step 2, 3, 4)
- Non-adherence to accounting and reporting requirements and standards (Step 1, 2, 3, 4)
- Poor debt management or excessive debt (Step 1, 2, 3, 4)
- Unauthorized transactions/ contracts made on behalf of Holcim (Step 1)

IMPACT
- Financial losses
- Errors in financials

CONTROL & FREQUENCY

1. **Approval according to local delegation of authority and Group Treasury Directive of any new financial instruments, borrowings, commitments and working capital schemes. *Upon Request***
2. **Sign-off by the CFO (or designee) of the list of all outstanding financial instruments, commitments and working capital schemes. *Quarterly***
3. **Countries trading in derivatives locally due to regulatory reasons, must have it reviewed by Treasurer (or designee) to reconcile the outstanding positions to counterparty statements. *Quarterly***
4. **Group Head of Treasury approval is granted for any cash pool limit increase (Cash pool participants and all entities in scope). Cash pool breaches are reported to the Head Group Treasury and corrective actions implemented within the agreed time frame. *Quarterly***

59 Financial instruments, borrowings, commitments and working capital schemes

REQUIREMENTS

- Financial instruments, borrowings, commitments (e.g. trade finance facilities, surety bonds, guarantees lines...) and working capital schemes (e.g. supply chain financing, factoring, off balance sheet inventory financing) and related disbursements can only be entered into after having been approved by appropriate personnel in accordance with local and Group Delegated Authorities and Group Treasury Directive. The Treasury Manager (or designated person) keeps track of all disbursements related to the repayment of borrowings and ensures that both the repayments and the related borrowings are properly recorded, including the recognition of current and non-current portions of the liabilities. (Step 1)
- Financing contracts have to be in line with the Holcim guide on loan documentation; any exception must be approved by Group Treasury. No financial covenants are accepted. Obtain Group Treasury approval for any financial contract not in line with the Holcim guide on loan documentation. (Step 1, 2)
- The list of all financial instruments, borrowings, commitments and working capital schemes must be supported by adequate documentation and signed off by the CFO (or designee) as well as reported as per the reporting guidelines. (Step 3)
- Third party and intercompany financing shall be renewed at least six months prior to maturity or earlier if required. (Step 3)
- Countries trading in derivatives locally due to regulatory reasons must quarterly reconcile the counterparties statements with the outstanding positions. Fair values are those indicated by Group Treasury. (Step 3)
- Cash pool limits are approved by Group Treasury. Cash pool drawings must remain within approved limits. Any potential cash pool limit breach shall be immediately reported to the Head Group Treasury and remediated with appropriate corrective actions. Corrective actions are implemented within the time frame agreed with Group Treasury. (Step 4)

Link to: Group Delegated Authorities (GDA), Finance Policy, Group Treasury Directive, HARP: 4.09 Financial Instruments, 3.1.5 Commitments, Contingencies and Guarantees , 3.1.2.1.13 for supply chain financing, factoring , 3.1.1.1.10 for off-balance sheet inventory financing, 3.1.1.1.2 Cash and Cash Equivalents, 3.1.1.1.4 Short-Term Financial Receivables, 3.1.2.1.02 Liabilities From Short-Term Financing, 3.1.1.2.3 Long-Term Financial Receivables, 3.1.2.2.2 Long-Term Financing Liabilities, 4.9.6.1 Credit Lines and Examples for Illustration Purposes,Treasury Information Management: 7.3.4.3.2, 7.3.4.3.3, 7.3.4.3.4 Credit Line Column Descriptions

60 Forex, interest rate, commodities risks monitoring and hedging

PRIMARY OBJECTIVE

Exposure to foreign exchange, interest and commodity risks are regularly reported and hedged according to the Group Treasury Directive.

RISK
- Improper management of foreign exchange (Step 1, 2)
- Improper management of interest rates risk (Step 1, 2)
- Increase in energy costs (incl. AFR) (Step 1, 2)

IMPACT
- Financial losses

CONTROL & FREQUENCY

1. **Monthly sign off and notification to Group treasury of the exposure in foreign currency and potential foreign exchange or interest rate exposure that may need to be hedged by Group Treasury.** ***Monthly***
2. **Review and approval by the CFO (or designee) of the consumption forecast used to hedge energy price exposure on a quarterly basis and notification to the Energy desk if there is any change in the underlying index used to procure the commodity.** ***Quarterly***

REQUIREMENTS

- Exposure to foreign exchange, interest risks are regularly reported and hedged according to the Group Treasury Directive and Foreign Exchange & Interest Rate Risk Management Directive. (Step 1)
- Foreign exchange, (FX), risks must be mitigated by natural hedging as much as possible. If not possible, it must be identified and managed to the maximum extent possible in cooperation with Group Treasury and in accordance with the Group Delegated Authorities (GDA). (Step 1)
- Speculation is strictly forbidden. Country financings and deposits are denominated in their functional currency whenever possible. Foreign exchange leasing is not allowed. Foreign exchange exposure must be identified and mitigated by natural hedging as much as possible. (Step 2)
- Exposure to commodity price risk is regularly followed up, hedged and reported according to the Financial Risk Directive for Energy. (Step 2)

Link to: Group Delegated Authorities (GDA), Finance Policy, Group Treasury Directive, Foreign Exchange (FX) & Interest Rate (IR) Risk Management Directive, Financial Risk for Energy Directive

Sustainability

61 Environmental impact

PRIMARY OBJECTIVE

Monitor and manage air emissions, water and waste to identify and address the environmental risks

RISK

- Air emissions (e.g. dust, Nox, Sox) exceeding authorized standards (Step 1)
- Excessive waste deposits and soil or water contamination (Step 1)
- Failure in quarry rehabilitation and biodiversity management (Step 1)
- Failure in water management (e.g. liquid effluents with detrimental impact on water resources) (Step 1)
- Deviation from CO_2 reduction standards (incl. internal Group targets) (Step 1)

IMPACT

- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

1. **Group monitoring and reporting requirements for air emissions (incl. CO2), waste, water management and people are followed and an annual management review to verify compliance with Group Policies, Directives and local regulations is conducted and action plans are documented by Plant Manager, and approved by the Country CEO.** ***Annual***

REQUIREMENTS

- All plants must have an environmental management system in place to ensure that all environmental impacts and risks are effectively managed and mitigated. Environment related permits (e.g. general environmental, emissions, water discharge, waste management) to be reviewed annually to ensure compliance.
- Environmental impacts have to be systematically identified according to the following steps:
  - Identify environmental aspects of activities, products and services over which plants have control and/or influence
  - Assess the risks linked to the identified environmental aspects that may have a significant impact
  - Maintain an up-to-date catalogue of significant environmental impacts during normal and abnormal operations
- Environmental impacts must be systematically managed to sustain and further improve environmental performance, while controlling environmental risks not only of our own operations, but including the supply chain. Progress must be monitored, evaluated and documented as required by the local regulations, or at least on an annual basis.
- For Cement plants, install and operate a continuous emission monitoring equipment for dust, nitrogen oxides (NOx) sulfur dioxide (SO2), Volatile Organic Compounds (VOC), carbon monoxide (CO) as per the Holcim Emission Monitoring and Reporting standard.
- Performance improvements on CO2 emissions, Water, Circular Economy and People must be aligned to commitments recorded in CEM Plant Development Plans (PDP) and other environmental roadmaps where applicable.
- Water and Waste must be managed preferring reuse and recycling to discharge and disposal, as per the the Circular Economy Policy, the Health, Safety and Environment (HSE) Internally Generated Waste standard and the Health, Safety and Environment Water Management Standard..
- All countries and operating plants must report at least yearly environmental data and KPIs in the Sustainable Reporting Campaign according to Holcim Environmental Reporting guidelines.
- Group Reporting Units (GRU) must report monthly Sustainability KPIs according to Group ARC instructions. Inaccuracy or incompleteness of the KPIs in SAP-FC must be disclosed in the financial certification package. Sustainable Development indicators reported to the Group are based on validated data source, calculation method, and are reviewed for reasonableness and validated by country sustainable development senior management on a half yearly basis.

Link to: Environmental Policy, S&E policy, Climate Policy, Nature Policy, Circular Economy Policy, Quarry Rehabilitation and Biodiversity Directive, Health, Safety and Environment Internally Generated Waste Standard, Health, Safety and Environment Water Management Standard, Sustainable Procurement Directive, Holcim Emission Monitoring and Reporting standard and Holcim Environmental Reporting guidelines.

62 Social impact: Human rights & Stakeholders

PRIMARY OBJECTIVE

Implement the Human Rights approach to identify, monitor and remediate Human rights-related risks and impacts in our operations, supply chain and with our business partners.

RISK
- Infringement of human rights standards (Step 1, 2, 3)
- Improper or insufficient stakeholders management (impact & value creation) (Step 4, 5)
- Ineffective or unethical vendor selection process (incl. TPDD process) (Step 1, 2, 3)
- Unauthorized transactions/ contracts made on behalf of Holcim (Step 5)
- Corruption and Bribery (Step 5)

IMPACT
- Compliance
- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

1. **Human Rights assessment is performed as per the Human Rights Directive and approved by the entity CEO within a timetable agreed with the Group Sustainability.** ***Annual***
2. **Human Rights & Stakeholder Engagement Action Plans, including human rights-related grievances, complaints and follow-up actions are reviewed and validated by the Local Executive Committee at least annually and signed off by the entity CEO.** ***Annual***
3. **Human Rights & Stakeholder Engagement Action Plan and other KPIs are submitted by the GRU via the Group reporting tool.** ***Annual***
4. **A stakeholder engagement & human rights action plan is deployed for all operational sites and the stakeholder mapping exists and are updated every year.** ***Annual***
5. **Social investments, inclusive business and donations are approved and documented according to Group guidelines and Group Delegated Authorities.** ***Upon Request***

REQUIREMENTS

All Group Reporting Units (GRUs) must ensure that the following 6 elements of the Human Rights Approach are in place according to Human Rights and Social Policy and Human Rights Directive:

- Identify Human Rights risks and impacts: a lead designated by the CEO conducts at least every 3 years a human rights assessment based on their risk level covering our own operations, suppliers, business partners and communities. (Step 1)
- Address adverse impacts: All assessments (impact or self) must result in a Human Rights and Stakeholder Engagement Action Plan that must be reviewed at least annually. Major risks or impacts must be immediately added to the Action Plan, addressed by local ExCo and reported to the relevant Group function(s). (Step 1)
- Grievance and remedy: A clear site-level mechanism (phone number, email address, etc.) for internal and external stakeholders to raise issues related to our operations exists and is managed by a function appointed by the entity ExCo. A record of all Human rights-related complaints must be kept and related follow-up actions are added in the Human Rights and Stakeholders Engagement Action Plan. (Step 2)
- Stakeholder Engagement: Every site must have a Stakeholder Map and a Human Rights & Stakeholder Engagement Action Plan managed at local level and updated at least annually. The Group Sustainability will approve the submitted Stakeholder Map and a Human Rights & Stakeholder Engagement Action Plan as per defined Group schedule. In cement plant and grinding unit, a Community Advisory Panel (CAP) must be in place. (Step 3).
- Monitor and communicate: Results of the Human Rights assessments, an up-to-date version of the implementation of the Human Rights and Stakeholder Engagement action plans and other Key Performance Indicators (KPIs) defined by Group Sustainability must be reported via the Group reporting system annually. (Step 4)
- Social initiatives are managed based on the local context and as per Group Delegated Authorities. (Step 5)

Link to: Group Delegated Authorities (GDA), Human Rights and Social Policy, Human Rights Directive, Strategic Social Investment, Sponsorship and Donations Directive, Sustainable Procurement Directive

Operational Technology (OT)

63 OT Security baseline controls for Cement Plants & Grinding Stations

PRIMARY OBJECTIVE

Reduce the risk of cyber attack on the Cement Plant OT systems.

RISK
- Successful cyber attack (IT/OT) (Step 1, 2, 3, 4, 5, 6, 7)
- Business disruption due to IT/OT unavailability (Steps 3, 5, 6, 7)
- Unauthorized access, disclosure, modification, damage or loss of data or the OT system (Step 1, 2, 3, 4, 5, 6, 7)
- Lack of industrial asset maintenance (Step 1, 2, 6, 7)

IMPACT
- Operational disruption
- Reputational damages
- Financial Losses
- Fraud

CONTROL & FREQUENCY

1. **OT roles and responsibilities per plant, region and global level are assigned. OT plant responsible and users are trained.** ***Annual***
2. **OT asset Inventory is quarterly reviewed and maintained in each plant. Upgrade / replacement plans are defined in consultation with and in line with the corporate strategy.** ***Quarterly***
3. **Secure network architecture is designed segregating IT and OT basic network zones (PCS, Industrial, Lab & DMZ) by using firewalls. Traffic flows between zones are controlled as per section 2.4. Wireless networks are restricted, unless hardened and secured as per section 2.3** ***Upon Change***
4. **Access is granted on need basis upon request being approved by plant manager or delegated person. Access rights are reviewed quarterly. Remote access connections from external networks must not connect directly to PCS, Industrial and Lab zones, but through DMZ zone or above. Technical measures are in place to authenticate, authorize, and monitor the remote access sessions.** ***Upon request***
5. **Annual verification that the technical measures are in place to prevent malicious code (anti-malware, anti-virus solutions). They are deployed on all the OT equipment connected to the OT networks. They are strictly following the guidance principles.** ***Annual***
6. **Backup & Restore procedures for OT each critical systems must be defined and documented including the need for offsite storage of backup.** ***Upon Change***
7. **Verify that OT equipments are placed in locations fulfilling physical and environment security requirements as per Section 4 of the standard.** ***Annual***

REQUIREMENTS

Note: Operational Technology (OT) Systems refers collectively to Cement Plant Industrial Applications and OT Infrastructure (Hardware, Operating System, Database, Network, Interfaces)

- Plant management responsibilities for compliance (section 10); the personnel having a logical and a physical access to an OT endpoints must attend the regular OT cybersecurity training while OT users should have general awareness training (section 7); basic OT Cyber Incident Response Roles & Responsibilities defined (section 6.2) - (Step 1)
- OT asset inventory requirements (section 6.3), patch management requirements (section 5.3), and the upgrade/replacement strategy (section 5.4) - (Step 2)
- The firewalls are installed and configured to effectively control and limit all the data traffic flows between IT and the OT zones as per Cement Plant IT/OT Security Group Standard - IT/OT network security requirements (sections 2.1, 2.2, 2.3 and 2.4) - (Step 3)
- The logical access management requirements in terms of user lifecycle, authentication and authorization as per section 3, including the management of all remote access connections to or from the company networks - (Step 4)
- All capable network enabled endpoints in the OT network zone (servers, workstations) should be protected against malicious code with network anti-malware technologies (section 5.2) - (Step 5)
- Documented backup procedure needs to be in place for each critical OT system (section 5.5) - (Step 6)
- OT equipment must be in locations fulfilling physical and environment security requirements (section 4). OT servers must be located in server rooms meeting OT Server Room Requirements - (Step 7)

Link to: IS_S14_Cement Plant IT/OT Security Group Standard, Minimal Control Standards for OT

Acronyms

Environmental, social, and governance (ESG)

Direct Debit (DD)

International Financial Reporting Standards (IFRS)

Request for Proposal (RfP)

Accounting, Reporting, Consolidation and Controlling (ARC)

Directors & Officers (D&O)

International Organization for Standardization (ISOs)

Risk with zero conflicts (RWZC)

Anti-Bribery and Corruption (ABC)

Data Universal Numbering System (DUNS)

Key Performance Indicators (KPIs)

SAP Bank Communication Manager (SAP-BCM)

Board of Directors (BoD)

Enterprise Resource Planning (ERP)

Holcim Accounting and Reporting Principles (HARP)

SAP Flexible Real Estate Management (RE-FX)

Business Resilience Team (BRT)

Flexible Real Estate Management (RE-FX)

Legal Entity Management Tool (Umbrella)

SAP Governance, Risk, and Compliance (SAP-GRC)

Business Service Centers (BSCs)

Foreign Exchange (Forex or FX)

Manual Journal Entries (MJEs)

SAP- Financial Consolidation (SAP-FC)

Capital expenditures (CAPEX)

Generally Accepted Accounting Principles (GAAP)

Mid-Term Plan (MTP)

Security & Resilience Management System (SRMS)

Cash-Generating Unit (CGU)

Group Delegated Authorities (GDA)

Minimum Control Standards (MCS)

Security Incident Notification Tool (SINT)

Change in structure (CIS)

Group Insurance and Risk Financing (GIRF)

Operating expenses (OPEX)

Security Services with Integrity (SSI)

Conflict of Interests (COI)

Group Level Material Risks (GLMRs)

Pension and Benefits Governance Team (PBGT)

Segregation of Duties (SoD)

Construction in Progress (CIP)

Group Reporting Unit (GRU)

People on Board (POB)

Senior Leaders Group (SLG)

Country Chief Executive Officer (CCEO)

Group Risk Insurance Tool (GRIT)

Personally identifiable information (PII)

Terrorist & Organised Crime (TOC)

Country Security Representative (CSR)

Group Treasury i/o Corporate Finance and Treasury (CFT)

Property Damage / Business Interruption (PDBI)

Third Party Due Diligence (TPDD)

Delegation of Authority (DoA)

Health, Safety and Environment (HSE)

Health & Safety Improvement Plan (HSIP)

Property, Plant and Equipment (PPE)

Third Party Liability (TPL)

Design Safety And Construction Quality Program (DSCQP)

Information Technology (IT)

Record to report (R2R)

Uncertain Tax Positions (UTPs)

Information Technology Service Centers (ITSCs)

Record to report (R2R)

Value Added Tax (VAT)

Holcim Ltd.
Group Internal Control
Grafenauweg 10
6300 Zug
Group.Internal-Control@holcim.com
www.holcim.com