MINIMUM CONTROL STANDARDS 2026

HOLCIM

INTRODUCTION

As a global leader in our industry, **Holcim upholds the highest standards** in managing and operating our business worldwide, recognizing this as an ethical responsibility.

We are committed to maintaining our license to operate by meeting the expectations of governments, authorities, employees, investors, and the communities we serve.

To achieve this, **Holcim ensures compliance with all local laws and regulations**, backed by a comprehensive set of **Minimum Control Standards (MCS) that all our countries and businesses must adhere to**, providing clear guidelines and accountability.

These **Minimum Control Standards are the capstone of our Corporate Governance framework**, covering 64 mandatory controls across key areas such as Governance and Compliance, Fixed Assets, Revenue, People, Inventory, Expenditure, Information Technology, Accounting and Consolidation, Tax, Treasury, Sustainability, and Operational Technology.

The implementation of these standards is **mandatory across our operations**. Every Holcim employee plays a vital role in executing the MCS and ensuring the effectiveness of our Internal Control System. It is essential that we engage our employees in the implementation process and establish the appropriate organizational structure to enhance control effectiveness.

Each year, the MCS are evaluated and tested across all our global operations. **Local CEOs and CFOs, and region management certify, through signed letters** to the Group, that these standards are in place and **operating effectively**.

Group Internal Control

MCS SUMMARY AND CONTENTS

	MCS	P.	Compliance	Reputational damages	Errors in financials	Operational disruption	Financial losses	Fraud
	PEOPLE	**53**						
25	Execution of onboarding, offboarding, master data management and transfers of workers	54	★	●	●		●	●
26	Payroll	57			●		●	
27	Compliance with payroll and local labor laws	58		●			●	
28	Employee pension and benefit plans	59			●		●	
	EXPENDITURE	**61**						
29	Management of supplier master data	62	★				●	●
30	Supplier qualification and performance evaluation	64	★	●			●	●
31	Three-way match, two-way match and direct vendor invoices	66			●		●	●
32	Payment processing	68	★	●	●		●	●
33	Accruals for expenditures not invoiced	70			●			
	INVENTORY	**73**						
34	Physical stock take of parts and supplies and materials, and volume reconciliations	75			●		●	●
35	Inventory valuation	80			●		●	●
	INFORMATION TECHNOLOGY	**81**						
36	Management of access to IT systems	82				●		●
37	Review of IT user access rights to production IT systems	83				●		●
38	Security configuration settings and batch job management	84				●		●
39	Data backup, storage and restoration process	85				●		●
40	Managing changes to IT systems	86				●		●

	MCS	P.	Compliance	Reputational damages	Errors in financials	Operational disruption	Financial losses	Fraud
	ACCOUNTING AND CONSOLIDATION	**89**						
41	Compliance with accounting and reporting standards, and extra-financial data disclosure	90		●	●			
42	Reconciliation of general ledger accounts	92			●			
43	Reconciliation of bank accounts	94			●		●	●
44	Reconciliation of intercompany balances	95			●		●	
45	Manual journal entries	97			●		●	●
46	Impairment of goodwill, intangible assets and tangible assets	98			●			
47	Transactions in a foreign currency	100			●			
48	Management of legal structure and consolidation hierarchy	101			●			
49	Consolidation of financial statements	103			●			
50	Statutory financial statements	104			●			
	TAX	**107**						
51	Tax risk assessment and reporting	108			●		●	
52	Tax filings and payments	109			●		●	
53	Deferred and current income tax calculations	110			●		●	
54	Transfer pricing	111			●		●	
55	Non-income (indirect) taxes	112			●		●	
	TREASURY	**113**						
56	Bank relations	114	★				●	●
57	Cash transactions are not permitted without Group approval	116	★				●	●
58	Secure payment means	118					●	●
59	Financial instruments, borrowings, commitments and working capital schemes	121			●		●	
60	Forex, interest rate, commodity risks monitoring and hedging	123					●	
	SUSTAINABILITY	**125**						
61	Environmental impact	126		●		●	●	
62	Social impact: human rights and stakeholders	128	★	●		●	●	
63	Climate change	130		●	●			
	OPERATIONAL TECHNOLOGY	**133**						
64	OT security baseline controls for cement plants and grinding stations	134		●		●	●	●

GOVERNANCE AND COMPLIANCE

1 Communication and promotion of the Code of Ethics and SpeakUp culture

PRIMARY OBJECTIVE

Senior management continuously communicates and role models the Code of Ethics while promoting a SpeakUp 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 AND FREQUENCY

1. The CEO must communicate the Code of Ethics and Integrity Line to all employees at least annually. Training must be delivered to high-risk employees in accordance with the training plan. Acknowledgements of the Code of Ethics from newly hired employees must be maintained by the People department (or designee). ***Annual***
2. Communication of the Code of Ethics for Suppliers to suppliers and outsourced service providers must be documented. ***Upon change***
3. Management must implement remediation actions for any confirmed breach. ***Upon request***

REQUIREMENTS

- The Code of Ethics must be communicated to all new employees during onboarding. New employees must acknowledge that they have read and understood the policy, and the acknowledgment must be stored in their personnel file. The method for obtaining and recording acknowledgments must be defined by the local Legal and People Departments (or designated department). (Step 1)
- The CEO must communicate at least annually, and more frequently as needed, to all employees regarding Holcim's values and the Code of Ethics, encouraging employees to speak up and report any suspected misconduct. (Step 1)
- Employees whose roles involve significant Code of Ethics risks or responsibilities for mitigating such risks (as defined by local Legal and Compliance) must complete periodic training as defined locally. (Step 1)
- The Integrity Line phone number must be operational from all facilities, and access to the website must be available through the company network. Posters promoting the Integrity Line must be displayed at all locations. The Integrity Line must also be communicated on the intranet, internet, and within or alongside the Code of Ethics for Suppliers. (Step 1)
- The organization's commitment to integrity and ethical behavior, as defined in the Code of Ethics for Suppliers, must be communicated to all suppliers and outsourced service providers. (Step 2)
- For existing suppliers, the commitment to the Code of Ethics for Suppliers must be documented through contractual terms and conditions included in purchase orders. For new suppliers, this commitment must be established during the tendering process. In all other contracts, best efforts must be made to include a clause recognizing the principles of anti-bribery, anti-corruption, and sanctions risk, either by referencing the Code of Ethics for Suppliers or using the standard template clause. (Step 2)
- In the event of a substantiated breach, remediation actions, including disciplinary measures, must be implemented in accordance with the SpeakUp and Investigations Remediation Guidance. The process must be initiated by the Case Manager (local or Group) and overseen by Group SpeakUp and Investigations. (Step 3)

Link to: Code of Ethics, Code of Ethics for Suppliers, Anti-Bribery and Corruption Policy, Compliance Policy, Human Rights and Social Policy, SpeakUp and Investigations Directive, Sanctions and Export Controls Directive, Human Rights Directive, Third Party Due Diligence Directive, Sustainable Procurement Directive, Responsible Lobbying and Advocacy Directive, Workers in the Value Chain Directive, SpeakUp and Investigations Remediation Guidance and Compliance Training Cycle Instructions

2 Compliance with Fair Competition laws and requirements

PRIMARY OBJECTIVE

Competition law risks are mitigated through adherence to the Group Fair Competition Directive, the Commercial Documentation Directive, and relevant legal guidance, with training provided to risk-exposed employees

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

IMPACT
- Compliance
- Reputational damages
- Financial losses

CONTROL AND FREQUENCY

1. Training on fair competition compliance for high- and medium-risk exposed employees must be completed and documented. Country-level trainings must be recorded by local Legal, and Group-level trainings must be recorded by Group Legal - Competition Law. ***Annual***
2. Pricing decisions, competitor contacts, and sources of market information must be documented in accordance with the Commercial Documentation Directive. Advice provided by Group Legal - Competition Law to local Legal departments and business stakeholders must also be documented. ***Upon request***

REQUIREMENTS

- Employees must comply with the Group Fair Competition Directive and all applicable local competition laws. (Step 1)
- All highly exposed employees must complete virtual or in-person fair competition training every two years. These trainings must be organized by the local Legal department or, at Group level, by Group Legal - Competition Law. Newly hired highly exposed employees must be trained within six months of joining the company. Participation in all trainings must be documented through a signed attendance list or other verifiable means (paper or electronic), with records retained by the local Legal department or, at Group level, by Group Legal - Competition Law. (Step 1)
- All medium-risk exposed employees must complete an e-learning training every two years. This training is provided by Group Legal - Competition Law to all local Legal departments. Newly hired medium-risk exposed employees must be trained within six months of joining the company. Successful completion of the e-learning training must be documented through an automatic certification generated by the e-learning tool or other verifiable means, with records retained by the local Legal department or, at Group level, by Group Legal - Competition Law. (Step 1)
- Employees must comply with the Commercial Documentation Directive to ensure that pricing decisions, competitor contacts, and sources of market information are properly documented. (Step 2)
- Group Legal - Competition Law must regularly provide advice to the local Legal departments and business stakeholders on competition law compliance through guidance papers or other appropriate means, as applicable. (Step 2)

Link to: Code of Ethics, Fair Competition Directive, Commercial Documentation Directive and SpeakUp and Investigations Remediation Guidance

3 Related party transactions and conflict of interests

PRIMARY OBJECTIVE

Related party transactions and conflicts of interest are properly reviewed and approved

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

IMPACT
- Compliance
- Reputational damages
- Financial losses
- Fraud

CONTROL AND FREQUENCY

1. Actual or potential conflict of interest situations reported by employees must be reviewed by the local Compliance Officer and approved by the Line Manager, in accordance with the Conflict of Interest Directive. All related actions or requirements must be documented and retained in the Holcim Integrity Gateway. ***Upon request***
2. An annual conflict of interest communication or awareness campaign must be conducted for the locally designated group of employees. ***Annual***
3. Any business deal or arrangement between a Group entity and a shareholder or a director's company must be reviewed and approved by the Legal department before initiation. ***Upon request***
4. The insiders' list of employees with access to privileged information on Holcim Ltd. must be maintained and managed at Group level by Legal and Compliance. Group Legal and Compliance must issue a quarterly communication, and the insiders' list must be cross-checked against the Hive users list. (Group level) ***Quarterly***
5. The insiders' list of employees with access to privileged information on a listed Group company must be maintained and managed at country level by the Legal or Company Secretarial department. The country Legal department must issue a quarterly communication. ***Quarterly***

3 Related party transactions and conflict of interests

REQUIREMENTS

- Employees must assess their own situations and disclose any actual or potential conflict of interest through the Holcim Integrity Gateway as soon as it becomes apparent. Disclosures must be reviewed in accordance with the Conflict of Interest Directive. (Step 1)
- Training on the Conflict of Interest Directive is mandatory for all employees and forms part of the standard compliance training program as defined in the Compliance Training Cycle instructions. (Step 2)
- Any business deal or arrangement between a Group entity and a shareholder or a director's company is considered a related-party transaction. For locally listed companies, related-party transactions must be reviewed by the Legal department prior to approval or signature. (Step 3)
- For Group privileged information, Group Legal and Compliance must maintain a list of all employees with access to such information. For other publicly listed entities, the entity Legal department must also maintain a list of employees with access to privileged information. These lists must be continuously updated. Once privileged information, such as consolidated financial or project data, becomes available internally, a communication reminding insiders of their obligation not to trade must be issued. The updated list, its previous versions, and related communications must be retained by Group Legal and Compliance or the applicable listed entity's Legal or Company Secretarial department. Access to the repository where these lists are securely stored must be restricted and controlled. (Step 4, 5)
- Group companies with securities listed on a stock exchange must adopt a binding Insider Dealing and Market Disclosure policy that establishes standards and processes at least equivalent to those required under applicable laws and regulations, ensuring compliance by the company, its directors, and employees. (Step 5)

Link to: Code of Ethics, Compliance Policy, Anti-Bribery and Corruption Policy, Insider and Management Transaction Directive, Conflict of Interest Directive and Compliance Training Cycle Instructions

4 Board of Directors secretarial requirements

PRIMARY OBJECTIVE

All local corporate legal requirements are fulfilled under the responsibility of the local Secretary and the Chairperson of the Board of Directors

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 AND FREQUENCY

1. The Chairperson and Secretary of the Board of Directors must sign a letter confirming compliance with all corporate legal requirements. ***Annual***

REQUIREMENTS

Where required by law, entities with a Board of Directors must ensure that all corporate secretarial duties are performed and documented in a timely manner in accordance with local requirements. On behalf of the Board of Directors, the Secretary and Chairperson must ensure that the Board of Directors and its committees (where applicable) operate in compliance with local corporate laws, the company's articles of incorporation, bylaws, charters, and other corporate governance regulations. This includes, in particular, that: (Step 1)

- Key corporate documents and records are maintained in accordance with applicable retention policies, local laws, and Group regulations.
- Meetings of the Board of Directors are held at least as frequently as required by local law.
- Minutes of Board of Directors meetings are recorded, approved, and maintained as part of the corporate records.
- Shareholder and Directors' registers are kept up to date.
- An annual shareholders' meeting is held, where applicable.
- All other local legal requirements must be observed. The designated Secretary must identify and document these requirements or liaise with the local Legal team to obtain and formalize them.
- The Chairperson and Secretary of the Board of Directors must jointly confirm compliance with all applicable corporate legal requirements by signing a compliance confirmation letter as part of the annual financial certification process. This control is considered achieved through the following alternative measures: 1) if the CEO is a member of the Board of Directors, a compliance confirmation letter signed by the CEO in their capacity as a Board of Directors member and by the Secretary; or 2) if the CEO is not a member of the Board of Directors, a compliance confirmation letter signed by the CEO and the Secretary, presented at a Board of Directors meeting with formalized meeting minutes signed by the Chairperson.

Link to: Group Delegated Authorities and Minimum Substance Requirements Directive

5 Health, Safety and Environment

PRIMARY OBJECTIVE

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

RISK
- Health and safety issue (injuries, fatalities, illness) or incident (Step 1)

IMPACT
- Reputational damages
- Operational disruption
- Financial losses

CONTROL AND FREQUENCY

1. The correct application of the Health, Safety and Environmental Policy must be verified annually by assessing the implementation of rewards and recognition, consequence management, completion of the Health, Safety and Environment Improvement Plan, employee and contractor training plans, Critical Controls, and Health, Safety and Environment key performance indicators. ***Annual***

REQUIREMENTS

Countries must ensure that the following four sections of the Health, Safety and Environment management system are established, operating effectively, and subject to regular review: (Step 1).

- Leadership and Engagement: A Rewards, Recognition, and Consequence Management program must be in place.
- Objectives, Planning, and Management Review: An annual Health, Safety and Environment Improvement Plan must be established in line with the Group process. Completion of the Health, Safety and Environment Improvement Plan must be tracked at the local Executive Committee level, while strategic areas must be tracked in the Group tracking tool.
- Operations and Support Processes: All employees and contractors must be included in the training plan, which must meet the minimum requirements for classroom and practical training as defined in the Health, Safety and Environment Standards. Countries must implement Critical Controls Management as defined by the Group.
- Performance Evaluation: A Group Health, Safety and Environment audit and annual self-assessment must be performed at unit level. Process Safety Management and Incident Reporting and Investigation processes must ensure incidents are correctly classified, and action plans are updated and implemented. Road key performance indicators must be reviewed.

Link to: Health, Safety and Environmental Policy, Sustainable Procurement Directive, Workers in the Value Chain Directive, Health, Safety and Environment Management System, Critical Controls Management and Group Health, Safety and Environment Intranet

6 Risk assessment

PRIMARY OBJECTIVE

A robust business and compliance risk assessment is performed and documented at least annually at the country or Service Center level

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 AND FREQUENCY

1. A risk assessment must be performed and documented annually in accordance with the Group Enterprise Risk Management process. Action plans must be defined and monitored for all high risks, at a minimum, in line with the Enterprise Risk Management guidelines. ***Annual***
2. Country and Service Center risk assessment reports must be signed off by the Country CEO and the Head of Service Center for their respective entities (electronically or physically) and submitted to Group Risk Management. ***Annual***

REQUIREMENTS

- Each country must appoint a Risk Lead to support local management in implementing the Enterprise Risk Management process and monitoring the effectiveness of mitigation measures. (Step 1)
- A risk assessment must be performed and signed off at least annually, identifying risks with the highest likelihood of occurrence and potential impact in line with the current Enterprise Risk Management methodology. Risks, local risk descriptions, likelihood (inherent and residual), financial and reputational impact (inherent and residual), mitigation measures, and action plans must be documented in the Enterprise Risk Management tool. Minutes of the presentation of the risk assessment to the local Executive Committee must be formalized and recorded by the Country Risk Lead. (Step 1, 2)
- Action plans must be defined for all high residual risks, at a minimum, in accordance with the Enterprise Risk Management guidelines. Each action plan's title, description, owner, and due date must be documented in the Enterprise Risk Management tool. (Step 1)
- The status of all action plans must be reviewed and updated in the Enterprise Risk Management tool as part of the annual Enterprise Risk Management process. (Step 1).

Link to: Finance Policy and Enterprise Risk Management Guidelines

7 Mitigation of business risks - Security

PRIMARY OBJECTIVE

Implement security measures and procedures in accordance with the Security Governance

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

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

CONTROL AND FREQUENCY

1. The Country CEO must annually sign off the country Security Risk Assessment and the country Security and Resilience Briefing. ***Annual***
2. Countries must implement the requirements of the Security Policy and the related directives, including Security, Security Services with Integrity, and Terrorism and Organized Crime. ***Annual***

REQUIREMENTS

- People and assets must be identified and mapped to support the Security Risk Assessment. (Step 1)
- A Security Risk Assessment must be conducted annually at the country level and every two years for Major Sites. (Step 1)
- A Country Security Representative must be appointed, and appropriate resources must be allocated to ensure effective execution of Security Governance. (Step 2)
- Mitigation controls must be implemented, and specific action plans and programs must be deployed for in-scope high and very high risks, as well as for Group level material risks. (Step 2)
- Travel-related risks must be identified and mitigated through proactive planning and approval processes. (Step 2)
- Suppliers providing security services must be engaged, managed, and evaluated in accordance with the Security Services with Integrity Directive and the Code of Ethics for Suppliers. (Step 2)
- Mandatory, risk-based security trainings and exercises must be completed and documented. (Step 2)
- All security incidents must be reported through the Group-approved tool, investigated as required, and followed by lessons learned and appropriate mitigation actions. (Step 2)

Link to: Security Policy, Code of Ethics for Suppliers, Security Directive, Security Services with Integrity Directive, Terrorist and Organised Crime Monitoring Program Directive, Travel and Events Directive and Workers in the Value Chain Directive

8 Mitigation of business risks - Group insurance

PRIMARY OBJECTIVE

Adequate risk coverage is ensured through adherence to the Group insurance process

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

IMPACT
- Financial losses

CONTROL AND FREQUENCY

1. Group insurance premiums must be paid before the due date. ***Annual***
2. Property insurance values must be reviewed and approved annually by the local Executive Committee (or designee) for accuracy, in accordance with Group methodology, to ensure replacement value coverage. ***Annual***
3. For all claims and losses covered by a Group insurance policy that are likely to exceed the applicable deductible or EUR 500,000 (or equivalent), an incident report must be submitted within 48 hours by the local Executive Committee (or designee) using the Group Claims Notification Forms. ***Upon request***
4. Group Insurance and Risk Financing must be informed: 1) before any new business activity is initiated, 2) of all capital expenditure projects exceeding EUR 5 million, and 3) of any Risk Improvement Actions not agreed upon by the country. ***Upon change***
5. The local Executive Committee must approve the purchase of any additional local insurance coverage for risks not included in a Group insurance program. ***Upon request***

8 Mitigation of business risks - Group insurance

REQUIREMENTS

- Countries must comply with the following five priorities:
  - Group insurance premiums must be paid by the due date without delay. (Step 1)
  - Property insurance values must be submitted annually to Group Insurance and Risk Financing before the due date to avoid under-insurance. (Step 2)
  - All claims and losses covered by a Group insurance policy that are likely to exceed the applicable deductible or EUR 500,000 (or equivalent) must be reported to Group Insurance and Risk Financing within 48 hours of the incident using the Group Claims Notification Forms. (Step 3)
  - All Risk Improvement Actions recommended by the insurer must be implemented within a reasonable timeframe. If the country does not agree with the Risk Improvement Actions, Group Insurance and Risk Financing must be notified, and alternative mitigation measures must be implemented. (Step 4)
  - Any business changes impacting Group insurance programs (e.g., new business activities such as installation of building materials or new products with different liability risks) must be communicated to Group Insurance and Risk Financing. (Step 4)
- All capital expenditure projects exceeding EUR 5 million (or equivalent) must be reported to Group Insurance and Risk Financing to ensure appropriate coverage. (Step 4)
- For risks not covered by Group insurance programs: (Step 5)
  - The local Executive Committee must arrange local insurance coverage as required by local regulations (e.g., motor liability, workers' compensation insurance).
  - The local Executive Committee may arrange additional local insurance for non-mandatory risks, provided these do not overlap with Group insurance programs (e.g., fiduciary insurance for local pension funds, trade credit insurance).

Group insurance programs:

- Property Damage / Business Interruption (PDBI), Commercial General Liability (CGL), Directors & Officers (D&O), Protection & Indemnity and Charterers Liability (P&I-C/L), Marine Cargo (MC), Terminal Operator's Liability (TOL), Environmental Impairment Liability (EIL) and Cyber Liability.
- Construction All Risk / Erection All Risk (CAR/EAR): Alternative local insurance allowed if cleared by Group Insurance and Risk Financing before project commences.
- Merger and Acquisition (M&A) related insurance programs as requested by the Group M&A team or for acquisitions with a target purchase value in excess of CHF 250 million.

Group Insurance and Risk Financing regularly reviews the risk landscape and reserves the right to define additional risks to be included under Group insurance programs.

Link to: Finance Policy, Group Insurance Directive, Capex Directive and Group Insurance Program Intranet

9 Mitigation of business risks - Business Resilience System

PRIMARY OBJECTIVE

A Business Resilience program is established and maintained in all countries to ensure preparedness, timely response, and effective recovery from disruptive events

RISK
- Supply chain disruption (Step 1)
- Business disruption due to IT/OT unavailability (Step 1)
- Attack against business asset (Step 1)
- Natural disaster (Step 1)
- Geopolitical tension (Step 1)

IMPACT
- Reputational damages
- Operational disruption
- Financial losses

CONTROL AND FREQUENCY

1. The implementation requirements of the Business Resilience Policy and Directive must be fulfilled at the country level. ***Annual***

REQUIREMENTS

- A Business Resilience Sponsor, Leader, and Coordinator must be nominated. (Step 1)
- A Business Resilience team with cross-functional representation must be established at both country and Major Site levels. (Step 1)
- A Business Resilience Plan ('Plan on a Page') must be maintained, documenting the Business Resilience team members, roles, and responsibilities. (Step 1)
- Risks emerging from the risk environment must be assessed using the applicable risk assessment methodology and tool. (Step 1)
- A Business Impact Analysis must be conducted to identify critical activities, recovery objectives, dependencies, points of failure, and contingency measures. (Step 1)
- Training and exercises must be conducted, and corresponding records maintained at both country and Major Site levels. (Step 1)
- Incidents that trigger activation of the Business Resilience team at the country or site level must be responded to, investigated, and reported in the Group-approved tool, as required. Lessons learned and mitigation actions must be identified and implemented. (Step 1)
- A Business Resilience Maturity Assessment must be completed. (Step 1)

Link to: Business Resilience Policy and Business Resilience Directive

10 Mitigation of business risks - Remediation of deficiencies and non-compliance with Minimum Control Standards

PRIMARY OBJECTIVE

A management process is established to identify and remediate deficiencies detected through the monitoring of the Minimum Control Standards (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 AND FREQUENCY

1. Local control designs that do not comply with the Minimum Control Standards central description and requirements must be approved by the Group Head of Function and Group Internal Control. Controls assessed as 'Not Applicable' must be validated by the Region Internal Control Correspondent. Deficiencies against the Minimum Control Standards must be approved by the Region Head (for countries) or Group Management (for functions) through the annual financial certification process. ***Annual***
2. The local Executive Committee must monitor the progress of all action plans related to Minimum Control Standards deficiencies to ensure timely resolution and reporting to the Group in accordance with Group Internal Control instructions. ***Half year***

REQUIREMENTS

Management must respond promptly and appropriately to deficiencies identified through monitoring activities and implement adequate and timely corrective actions. This process includes:

- MCS exception approval process: When a country is unable to design a local control description in compliance with the Minimum Control Standards requirements, the Country Internal Control Manager, after alignment with the Region Internal Control Correspondent, must use the MCS Design and Implementation Non-Compliance Approval process to obtain Group approval. The submission must be completed at least two weeks before the Control Design Assessment (CDA) deadline. All approvals must be recorded and made available in SAP Governance, Risk, and Compliance (GRC). (Step 1)
- Controls rated as 'Not Applicable' and the allocation of responsibilities between entities and Service Centers must be formally validated by the Region Internal Control Correspondent. (Step 1)
- Deficiencies against the Minimum Control Standards must be validated by local management and approved by the Region Head (for countries) or Group Management (for functions) through the annual financial certification process. (Step1)
- Any deficiency related to Minimum Control Standards classified as having an impact on compliance, including MCS 01, 02, 03, 06, 10, 11, 16, 20, 22, 25, 29, 30, 32, 56, 57, 62. (i.e., MCS 01.01/02/03; MCS 02.01/02; MCS 03.01/02/03/04/05; MCS 06.01/02, MCS 10.01/02; MCS 11.01/02; MCS 16.01/02/03/04; MCS 20.01/02; MCS 22.02, MCS 25.01; MCS 29.01; MCS 30.01/02; MCS 32.01/02; MCS 56.02; MCS 57.01, MCS 62.05) must be approved by the Region Compliance Officer (for countries) or the Chief Compliance Officer (for functions) prior to the signature of the annual financial certification. (Step 1)
- A root cause analysis, a detailed description of the deficiency, and an action plan to remediate any identified weakness must be performed and documented. (Step 2)
- Deficiencies must be communicated to the parties responsible for implementing corrective actions. (Step 2)
- Corrective actions and their progress toward completion must be regularly monitored and followed up. (Step 2)
- Action plans related to deficiencies must be tracked regularly by the local Executive Committee and Group Internal Control, at least twice per year. (Step 2)
- All deficiencies and related action plans must be tracked in SAP Governance, Risk, and Compliance (GRC). (Step 2)

Link to: Finance Policy, MCS Design and Implementation Non-Compliance Approval Process in AODocs, Internal Control Instructions and Holcim Financial Certification Permanent Instructions

11 Personal data protection

PRIMARY OBJECTIVE

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

RISK

- Unauthorized use of company and 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 AND FREQUENCY

1. Employees in scope must be trained, in accordance with the country-defined training cycle, on compliance with local data protection laws and regulations, and on how to recognize and report data breaches. ***Upon request***

2. Data Subject Consent Forms must be implemented, in local language where required, for different categories of data subjects (e.g., candidates, employees, customers, suppliers) in accordance with local data protection laws. Each department must annually verify that Data Processing Agreements are signed with all vendors processing personal data on behalf of Holcim. ***Annual***

REQUIREMENTS

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

- The data privacy notice or policy must be made available to all existing employees and distributed to new employees during the onboarding process. (Step 1)
- Relevant employees must be trained to recognize and report data breaches or any incidents relating to personal data which may carry reporting or notification obligations. Each country may determine which employees are considered relevant. (Step 1)
- Define a compliance training program for a locally determined cycle. Each country must specify the trainings to be delivered, the target population, and the applicable time period. All newly recruited relevant employees must complete the training within six months of joining Holcim. (Step 1)
- Seek advice from the Data Protection responsible person at Legal and Compliance, if necessary. (Step 1, 2)
- Consent must be collected and recorded when the employee's image (photo or video) is taken or used by the company. (Step 2)
- Data privacy notice or policy must be made available or distributed to all existing and new customers, as well as prospects, through one or more of the following communications channels: email, online customer platform, Holcim country website, an addendum to the existing commercial contract, or within the general terms and conditions of the commercial agreement. (Step 2)
- Customer's consent must be collected and recorded whenever required. Seek advice from the Data Protection responsible person at Legal and Compliance concerning the collection of customer consents. (Step 2)
- Seek advice from the Data Protection responsible person in Legal and Compliance when external vendors have access to personal data or PII handled by a Holcim entity. The advice should concern the implementation of an agreement with the vendors regarding the processing and protection of such personal data or PII. (Step 2)
- A process must be established 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 person in Legal and Compliance on how to respond to such requests. (Step 2)

Link to: Compliance Policy, General Data Protection Directive and 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 AND FREQUENCY

1. IT Service Centers must annually review and validate the segregation of duties rules established for ERP systems and critical business applications by region, and provide confirmation to the respective countries, functions, and Service Centers. ***Annual***
2. Segregation of duties reports for ERP systems and critical business applications must be reviewed at least semi-annually by the respective business process owners and the CFO (or designee). Any identified segregation of duties conflicts must be removed or mitigated in accordance with Group requirements. ***Half year***
3. User access levels for all critical business applications must be validated at least semi-annually. Any required corrective actions must be implemented within one month following the review. ***Half year***
4. Access for dormant users must be validated at least semi-annually to ensure it has been deleted or revoked. Any required corrective actions must be implemented within one month following the review. ***Half year***

REQUIREMENTS

Segregation of Duties:

- IT Service Centers must annually review the segregation of duties rule set for the ERP system and other regionally scoped applications to ensure alignment with Group rules. Local customized objects (transactions) must be updated with support from the business, and confirmation provided to the countries, functions, and Service Centers. Where the segregation of duties rule set is managed directly by the countries, the review must be performed at the country level. (Step 1)
- Risks with zero conflicts (RWZC) must be eliminated upon identification. No tolerance is allowed for conflicts associated with risks mapped as RWZC. (Step 2)
- Other segregation of duties risks (non-RWZC) must be kept to a minimum. Where removal is not possible, they must be mitigated through the implementation of compensating controls. These compensating controls must be documented and monitored to ensure they effectively reduce the identified risk. The operating effectiveness of the compensating controls must also be tested. (Step 2)
- Exceptions to the requirements set for RWZC and non-RWZC must be reviewed and agreed with the Region Internal Control Correspondent and approved by the Group Head of Internal Control. (Step 2)

Business Access Review:

At least twice a year, the following occurs for all critical business applications:

- A review of all user accounts must be performed to ensure that users have access appropriate to their job roles. Any excessive access not required for the performance of their job role must be revoked within one month from the date of identification. (Step 3)
- With support from IT, a report must be extracted listing all business users and their level of access, for the business to review and ensure that access rights are aligned with each user's job role. Business must propose corrective actions (e.g., revoking or changing access and sending a request to IT for implementation), to be supported by the IT team. (Step 3)
- Businesses must obtain the dormant user report from IT for all critical business applications and review it to ensure that access for dormant users is revoked or deleted in a timely manner. IT must be notified to disable or delete dormant user IDs accordingly. (Step 4)

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

Link to: Finance Policy, Annex 09: IT Controls, Annex 09.02: TIS Roles and Security Management, Annex 10: Holcim Segregation of Duties Conflicts (RWZC), and Annex 10.02: Holcim SAP Segregation of Duties Rule Set

13 Delegation of authorities and approval workflows

PRIMARY OBJECTIVE

A clear delegation of authority is defined in compliance with the Group Delegated Authorities and supported by an adequate approval system

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

IMPACT
- Errors in financials
- Financial losses

CONTROL AND FREQUENCY

1. The authorization policy, incorporating the requirements of the Group Delegated Authorities, must be approved by the local Executive Committee and, where applicable, by the Board of Directors. ***Annual***
2. Any contractual commitment entered into by the company and covered by the Group Delegated Authorities must bear the dual signatures of the authorized persons as defined in the local delegation of authority. ***Upon request***
3. The responsible manager must review and approve the workflow approval matrix (system-based or manual) to ensure compliance with the authorization policy. For manual approval processes, the documentation method must be defined, and evidence of each approval must be maintained. ***Half year***
4. The responsible manager must verify, at least semi-annually, the users configured in the approval workflows of the ERP system (e.g., users mapped to release groups). Any exceptions identified must be investigated. Users with authorization to update release groups must be reviewed, and any errors analyzed and corrected. ***Half year***

REQUIREMENTS

Group Delegated Authorities:
The Group define the approving authority and thresholds for key transactions and commitments involving Holcim or any of its subsidiaries. Countries and functions must operate within this framework, ensure compliance with these rules, and maintain proper documentation for all approvals. (Step 1, 2)

Defining the local delegation of authority: (Step 1, 2)

- An authorization policy or delegation of authority matrix must be established to define clear approval lines for all key transactions within monetary limits and other authorizations in the country, including signing authorities. As monetary thresholds increase, additional approvals from higher management levels are required, with the highest thresholds subject to approval by the Board of Directors and the Executive Committee. The local delegation of authority must be formally documented, kept up to date, and approved by the local Executive Committee and, where applicable, the Board of Directors.
- Group Delegated Authorities must be adhered to within the local delegation of authority matrix. Country authorities and thresholds defined in the Group Delegated Authorities may be delegated locally; such delegations must be documented in the local delegation of authority and approved by the local Executive Committee and, where applicable, the Board of Directors.
- Responsibilities must be clearly defined and communicated within the organization.
- Responsibilities, including those assigned to third-party service providers performing activities on behalf of the organization, must be clearly defined, specifying the extent of their decision-making authority.
- The local delegation of authority must be strictly followed for all transactions requiring approval.
- The local delegation of authority must be reviewed at least annually to ensure compliance with the authorization policy and defined limits, and updated as necessary.

Maintaining the delegation of authority in the system: (Step 3, 4)

- The local delegation of authority must be maintained in the ERP system workflow approval matrix. Initial setup and any subsequent changes must be supported by appropriate documentation and approved accordingly.
- At least semi-annually, a report of all users configured in the release groups (authorized approvers) must be generated and verified against the approved local delegation of authority, ensuring alignment with the Group Delegated Authorities. The report must be reviewed and signed off by the responsible manager.
- Access to update release groups must be restricted to authorized users only.

Link to: Group Delegated Authorities, Finance Policy, Brand Governance Directive and Minimum Substance Requirements Directive

14 Litigation disputes

PRIMARY OBJECTIVE

Risks arising from legal disputes are evaluated, and Group-relevant cases are recorded on a quarterly basis in the Group Litigation Management tool

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

IMPACT
- Errors in financials
- Financial losses

CONTROL AND FREQUENCY

1. The local Head of Legal (or designee) reviews and approves, on a quarterly basis, the information reported in the Group Litigation Management tool to ensure it is complete, up to date, and aligned with Group Legal requirements. ***Quarterly***

2. The Country CFO (or designee) performs a quarterly review of the provisions recorded in the Group Litigation Management tool to ensure consistency with the amounts reflected in the financial statements. ***Quarterly***

REQUIREMENTS

- The Legal department maintains and updates the status of all ongoing disputes, ensuring that the estimated maximum risk, expected risk, risk classification (probable, possible, or remote), and related provisions recorded in the financial statements are properly completed. (Step 1)
- At least once per year (typically at year-end), legal opinion letters must be requested for the most significant disputes, in particular those where external auditors require a third-party legal opinion or where the country Legal department is not able to make clear assumptions on the case outcome. The purpose is to ensure that the information on such cases is updated and properly validated. The legal opinions obtained are reviewed by the Legal department and the Country CFO. (Step 1)
- The Group Litigation Management tool is updated in line with Group Legal reporting requirements. At a minimum, provision amounts and risk classifications recorded in the tool must correspond with the financial statements at that date. The estimated maximum risk, risk classification, and provisions are reviewed by the Country CFO. (Step 2)
- The control is performed at least quarterly, at closing, and is required as part of the annual financial certification process. (Step 2).

Link to: Group Delegated Authorities, Data Retention and Deletion Directive and Group Litigation Management Tool

15 Review of contracts by Finance

PRIMARY OBJECTIVE

Contracts and material commitments are reviewed by Finance

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

IMPACT
- Errors in financials
- Financial losses

CONTROL AND FREQUENCY

1. The CFO (or designee) reviews and approves contracts in foreign currencies, leases, and all material commitments prior to signing or when subsequently amended, to ensure proper accounting treatment, appropriate foreign exchange risk management, and accurate disclosure. ***Upon request***

2. The CFO approves the accounting treatment of significant leases, in line with locally defined thresholds and the Group Lease Directive, including material, complex, and judgmental contracts. ***Upon request***

15 Review of contracts by Finance

REQUIREMENTS

- Each entity defines the scope and criteria for contracts subject to review by local Finance, based on the country's materiality thresholds as per SAP Financial Consolidation report P780-050. For leases, the Group Lease Directive applies. (Step 1, 2)
- Contracts are reviewed by the relevant Finance department prior to signing to ensure that: (Step 1, 2)
  - Contracts denominated in a foreign currency are communicated to the local Finance department and approved by the CFO (or designee) before signature.
  - Financial impacts are properly assessed and considered in the decision-making process (e.g., capital expenditures, operating expenses, IFRS 16 leases, take-or-pay and off-balance sheet clauses, power purchase agreements, hedging costs, etc.).
  - All material commitments are communicated to Group Finance to ensure proper accounting and disclosure, particularly for the Group's external reporting.
  - For IFRS 16, before signing, leases are formally approved according to the thresholds and approvers defined in the Group Lease Directive to ensure accuracy of contract data and valuation parameters (interest rates, probable end date, etc.). Countries must avoid leases generating foreign exchange exposure. Leases not denominated in the functional currency of the country require separate approval from Group Treasury, irrespective of whether they are budgeted.
  - Contracts related to control assessment or scope of consolidation (e.g., acquisition or divestment agreements, put or call option contracts, shareholders' agreements) are reviewed and communicated to Group Finance in accordance with HARP 4.1.5.3.
- During the Request for Proposal process, a financial review is performed to support the buy-or-lease decision, including an assessment of the financing method by Treasury experts and the potential financial statement impacts by Accounting experts, in line with the guidelines set in the Group Lease Directive. (Step 1, 2)
- In cases of volume increases or scope changes during the term of a contract involving foreign currency, all modifications must be communicated to Finance for appropriate follow-up and action. (Step 1, 2)

Link to: Group Delegated Authorities, Finance Policy, Procurement Policy, Lease Directive, Capex Directive, Treasury Directive, HARP 4.2.1 4.2.1 Accounting for Leases under IFRS 16 and HARP 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 the validity, proper filing, and timely renewal of all 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 AND FREQUENCY

1. The relevant local Executive Committee member annually reviews and approves the list of all permits and licenses required for business operations, with the Country CEO signing off on any exceptions or identified issues. ***Annual***

2. The country Legal team, together with the Quarry (Mine Planner) and Land Management Officer (or their equivalents), must annually review and approve all existing ownership titles, mining and surface rights, concessions, and permits, including those due for renewal. ***Annual***

3. The Land Management Officer (or equivalent), jointly with Quarry Management, must semi-annually review and approve the land ownership situation, including any proposed or planned land activities (e.g., acquisitions or disposals) and their impact on the relevant licenses. ***Half year***

4. The relevant stakeholders must annually review and approve the progress of mining activities and confirm compliance with mining regulations and permit requirements. ***Annual***

REQUIREMENTS

- For all relevant permits and licenses (e.g., environmental, archeological, operating, quarry and mining, production, energy use, vessels and ports, construction, air, water, deforestation, blasting, explosives handling and storage), roles and responsibilities must be clearly defined within the organization. Adequate processes must be established to ensure their validity, proper filing and archiving, timely renewal, and publication (where required). The list of permits and licenses must be kept up to date, with clear ownership assigned and a defined procedure in place for managing each permit and license type. (Step 1)
- Local laws and regulations, applicable international standards, and the Code of Ethics must be complied with in the management of all permit- and license-related activities. (Step 1)
- Third-party interactions with public officials for the acquisition, renewal, or review of titles, licenses, and permits must be managed through the Holcim Integrity Gateway. (Controls related to Third Party Due Diligence are covered in MCS 30.) (Step 1)
- All existing ownership titles, mining and surface rights, concessions, and permits must be reviewed at least annually by the country Legal team (or equivalent), in consultation with the Quarry (Mine Planner) and Land Management Officer, to ensure their validity. (Step 2)
- The Land Management Officer must lead a review of the land ownership situation twice a year (or as required by local regulations). Reviews of planned land acquisitions or disposals must be conducted jointly by the Land Management Officer, Quarry Management, and the country's raw material competent person. These reviews must cover all requirements necessary to maintain the validity of relevant licenses and permits. (Step 3)
- The renewal, activation, and exercise of mining rights and permits must be completed before their expiration date. (Step 3)
- Meetings with all relevant stakeholders, including Quarry and Plant Management, Sustainable Development, Environment, Legal, and Land Management, must be conducted to review the progress of mining activities and to monitor compliance with mining regulations and permitting obligations. (Step 4)

Link to: Code of Ethics, Third Party Due Diligence Directive, Technical Recommendation: Land Management and 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, and that restoration and rehabilitation obligations for all applicable sites are implemented and accurately reflected in the 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, reporting requirements and standards (Step 2)
- Inaccurate or fraudulent closing entries (incl. judgemental assumptions and estimates) (Step 4)

IMPACT
- Reputational damages
- Errors in financials
- Operational disruption

CONTROL AND FREQUENCY

1. An annual reconciliation of resources and reserves with the total extracted tonnages must be performed and communicated to the Accounting department, based on yearly estimates and approved by the Country CFO. Instances where the remaining useful life of plants and equipment exceeds the remaining secured reserves must be reported as part of the annual financial certification process. ***Annual***
2. Finance and Land and Quarry Management must annually verify the validity of the restoration and rehabilitation concepts, associated costs, and the assumptions used to calculate the related provisions. ***Annual***
3. Each quarry must be assessed to determine whether it is classified as having high biodiversity importance (BIC 1 or BIC 2). For such sites, an annual review of the Biodiversity Management Plan must be conducted by a qualified expert to ensure that implemented actions adequately address site-specific biodiversity issues. The Biodiversity Indicator and Reporting System must be established for all quarries. ***Annual***
4. The Legal department must review and validate all contracts related to restoration and rehabilitation works prior to signing. ***Upon request***

REQUIREMENTS

- Reserves for cement production sites must be classified in accordance with the Raw Material Resources and Reserves Reporting Standard. Annually, raw material resources, reserves, and raw mix lifetime figures must be reviewed and validated by a Holcim competent person and reported in line with the business cycle requirements defined in the Plant Development Plans, as per the Raw Material Resources and Reserves Reporting Standard. (Step 1)
- Aggregates resources and reserves must be classified according to HARP definitions. Each country must report annually on raw material resources and reserves in accordance with the business cycle requirements established by Aggregates Reserves Management. (Step 1)
- The yearly reserve estimates must be reconciled with the total extracted tonnages reported to the Accounting department. (Step 1)
- All acquired resources and reserves must be accurately recorded in the accounts and assessed to ensure no impairment issues arise. For cement and aggregates sites where the useful life of plants and equipment exceeds the remaining secured reserves or production lifetime, appropriate action plans must be developed and reported as part of the annual financial certification process. (Step 1)
- A restoration and rehabilitation plan must be developed in line with Group requirements, covering the dismantling and removal of plant and equipment, the restoration of sites where such assets are located, and the rehabilitation of each quarry operation. The plan must align with the long-term development objectives of the site and clearly define the scope, magnitude, and timeline of the restoration or rehabilitation activities. The plan and its supporting documentation must be available to Land and Quarry Management as well as Finance. (Step 2)
- The cost of restoration and rehabilitation work, determined using local historical data or estimates from recognized specialists, must be verified and approved by the country Plant Management. These cost estimates must be included as an annex to the restoration and rehabilitation plan to allow verification of the underlying assumptions. (Step 2)
- At least once a year, Finance and Land and Quarry Management, with Legal involvement where necessary, must meet to review the validity of the restoration and rehabilitation concept, assess the related cost estimates, and validate the assumptions used in calculating site restoration and rehabilitation provisions (e.g., discount rate, timing of future cash flows, residual life, etc.). If any revision affects a legal guarantee related to restoration or rehabilitation, Finance must ensure that the corresponding adjustment is secured. (Step 2)
- A Biodiversity Management Plan must be established and maintained for all quarries classified as having high biodiversity importance (BIC 1 or BIC 2). (Step 3)
- A Biodiversity Indicator and Reporting System must be implemented for all quarries (active, non-active, and closed) and conducted in accordance with the criteria and frequency defined in the Quarry Rehabilitation and Biodiversity Directive. (Step 3)
- Materials used for restoration and rehabilitation activities must comply with the Health, Safety and Environment (HSE) Internally Generated Waste Standard. (Step 4)
- Restoration and rehabilitation work contracts must be reviewed by Legal experts for regulatory compliance prior to signing and copied to Finance for proper filing. (Step 4)

Link to: Finance Policy, Quarry Rehabilitation and Biodiversity Directive, Lease Directive, Capex Directive, Raw Material Resources and Reserves Reporting Standard, Health, Safety and Environment (HSE) Internally Generated Waste Standard, Aggregates Reserves Management (ARM), Criteria for Biodiversity Importance Category (BIC 1 and 2), HARP 4.10.2 Site Restoration, HARP 6.6.5.2 Raw Material Resources, HARP 6.6.5.3 Raw Material Reserves, HARP 60.6.5.05 Reserves Life [yrs] (for Aggregates business), HARP 4.10.2 Site Restoration (accounting), HARP 4.10.3 Amortization of Raw Material Reserves (accounting), HARP 3.1.8.2 Classification of CAPEX (classification and reporting), HARP 4.2.1 Accounting for Leases under IFRS 16 (specific exemptions related to reserves when Holcim rents the land), and HARP 3.2.1.2.28 Depreciation and Amortization of Long-Term Operating Assets (depreciation of raw material reserves and capitalized mining concessions)

18 Classification and depreciation of fixed assets

PRIMARY OBJECTIVE

Ensure accurate 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, 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 AND FREQUENCY

1. The appropriate Finance representative must approve the capitalization of expenditures in accordance with HARP classifications and ensure the correct asset life and depreciation method are applied. ***Quarterly***

2. The appropriate Finance representative must review and approve Construction in Progress accounts on a quarterly basis to ensure that only active projects are included. Non-viable projects must be written off, and completed projects must be transferred to Property, Plant and Equipment. ***Quarterly***

3. The CFO (or designee) must approve the write-off of all unused, mothballed, or idle assets, as well as any changes to the depreciation method applied. ***Upon request***

REQUIREMENTS

- Assets must be properly classified in accordance with HARP 3.1.1.2.4 Property, Plant and Equipment (PPE), HARP 4.4 Capitalization, Accounting and Valuation of Assets, and HARP 4.2 Accounting for Leases, as well as the Lease Directive and the CAPEX Directive. (Step 1)
- Depreciation schedules required for various reporting purposes must be maintained in accordance with HARP 3.2.3.5 Ordinary Depreciation and Amortization, and HARP 4.4.4 Useful Lives of Property, Plant and Equipment. (Step 1)
- For mineral reserves, refer to HARP 3.1.1.2.4 Property, Plant and Equipment (PPE), Section 3 - Land and Mineral Reserves. (Step 1)
- The capitalization of expenditures and the timely commencement of depreciation must be reviewed and approved by the appropriate Finance representative. Any related journal entries must include supporting calculations and be signed off by the appropriate Finance representative in accordance with MCS 45. (Step 1)
- The responsible person must review the status of all Construction in Progress assets to determine whether assets with recoverable value are ready for use. Any project changes or variations in asset utilization must be considered when assessing potential impairment. Based on this review, the Finance representative responsible for Property, Plant and Equipment must reclassify Construction in Progress to fixed assets and initiate depreciation within thirty days of the recorded completion date.

All related journal entries must be reviewed to ensure proper classification and approval, in accordance with HARP 3.1.1.2.4 Property, Plant and Equipment (PPE). (Step 2)

- Accelerated depreciation must be applied when a tangible asset becomes obsolete, is replaced earlier than expected, or can no longer be used due to newly implemented environmental requirements. (Step 3)
- Once assets are identified as unused, mothballed, or idle, the related depreciation and underlying assumptions must be supported by adequate documentation and approved by the CFO (or designee). The write-off of unused, mothballed, or idle assets, as well as any changes to the depreciation method (including reductions in useful life), must also be properly documented and approved by the CFO. Refer to HARP G 002-13 Mothballing and Plant Closure in HARP 3.1.1.2.4 Property, Plant and Equipment (PPE) (section 2.10 Idle Assets). (Step 3)
- Group Sustainability targets may lead to additional investments in proven technologies, causing certain assets to become idle or obsolete earlier than their originally estimated useful lives. Such cases must be carefully reviewed with the Region Head of Finance, and accelerated depreciation must be applied where appropriate. (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

Ensure the accuracy and completeness of fixed asset balances in the financial statements through periodic verification

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

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL AND FREQUENCY

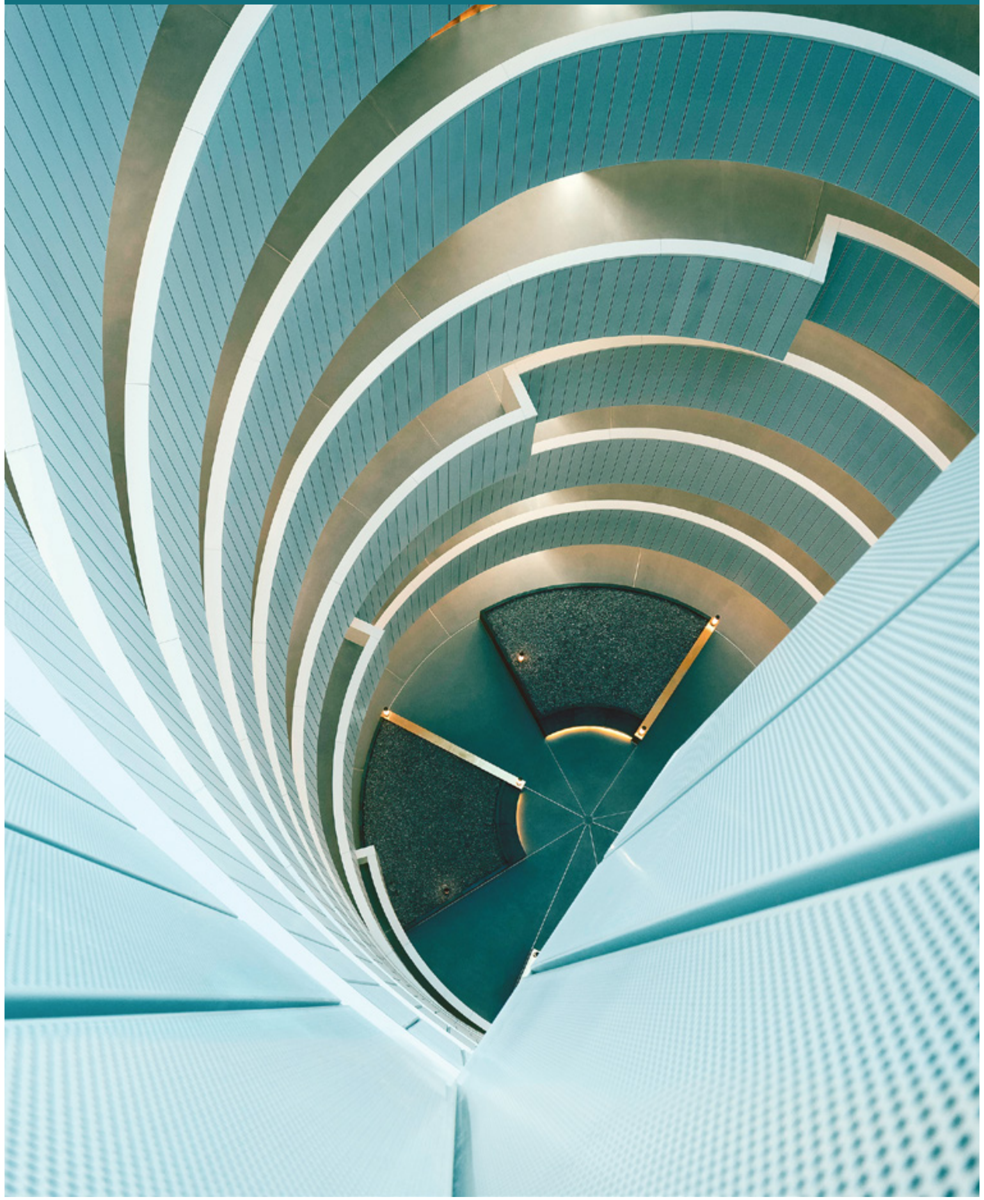
1. A complete physical inventory count of fixed assets must be conducted at least once every three years, with all counts properly documented. Any discrepancies identified must be adjusted following approval by the CFO. ***Annual***

REQUIREMENTS

- Regular physical inventory counts of fixed assets must be carried out on a rolling basis (at least once every three years). Differences identified through floor-to-list and list-to-floor comparisons must be analyzed to determine root causes and corrective actions. (Step 1)
- Any adjustments must be properly documented and approved by the CFO before recording. (Step 1)

Link to: Finance Policy

REVENUE



20 Management of customer and material master data

PRIMARY OBJECTIVE

Ensure that 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 AND FREQUENCY

1. Countries must determine whether sanctions screening is required for any new customer to ensure the customer is not a sanctioned person and does not present sanctions-related risks. Where required, the screening must be performed and documented locally. ***Upon request***
2. Changes to customer master data must be based on approved requests and performed only by authorized users. A quarterly review and sign-off by the responsible manager must be conducted on a minimum of twenty-five random samples to ensure that such changes were based on approved requests and performed by authorized users. ***Quarterly***
3. Annually extract a list of inactive customers to ensure they are blocked or deactivated. Any exceptions must be documented and approved by the responsible manager identified locally. ***Annual***
4. A quarterly verification and sign-off by the responsible manager must be performed to ensure that only users from the Customer Master Data Management function have access to change customer master data. ***Quarterly***
5. Changes to material master must be based on approved requests and performed only by authorized users. A quarterly review and sign-off by the responsible manager must be conducted on a minimum of twenty-five random samples to ensure that such changes were based on approved requests and performed by authorized users. ***Quarterly***
6. A quarterly verification and sign-off by the responsible manager must be performed to ensure that only users from the Material Master Data Management function have access to change material master data. ***Quarterly***

REQUIREMENTS

- Before creating a new customer in countries identified as having sanctions risk, a sanctions screening (or exemption) must be obtained from local or region Compliance or approved by the Sanctions Board, as required. Sanctioned entities or individuals must not be added to the customer master data. Ongoing sanctions screening must be performed in accordance with the Sanctions and Export Controls Directive, systematically as defined in the Trade Compliance Management tool, and at the transaction level for the defined transactions in scope. (Step 1)
- The creation of a new material, as well as any subsequent changes, must be approved in accordance with a predefined approval process or framework, supported by appropriate documentation. A verification must be performed to ensure that all required information is complete. (Step 2)
- The addition of a new customer and any subsequent changes require approval based on a predefined process with appropriate supporting documentation. As a minimum, documentation supporting the customer's identity is required. One of the following examples is sufficient: certificate of incorporation or registration, extract from commercial register, business license, tax certificate, Data Universal Numbering System certificate, or a 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 it is required when a refund or subsequent change to bank record is to be processed. One of the following examples is sufficient: RIB, IBAN, a bank letter of confirmation, a canceled cheque displaying the customer's name, a bank statement, or other acceptable documentation establishing the link between the customer identity and the bank details. A check is performed to confirm that all required information is completed. Regional specificities must be aligned with the Region Internal Control Correspondent. (Step 2)
- For existing customers, changes to bank information in the customer master data must be performed only after completion of the callback process. The process must be documented, including a post-confirmation email verifying that the callback was conducted. (Step 2)
- Quarterly, a master data change report must be generated, covering all creations, modifications, and deletions, to ensure that all changes were duly approved and performed by authorized users. Any exceptions identified must be documented and reported immediately for investigation. Corrective actions must be documented and tracked. All exceptions are closed within the locally defined timeframe. As a minimum, the following fields should be considered critical in SAP:
  - For customer master data: Customer name, Value Added Tax (VAT), bank details (as defined above), reconciliation account, account assignment group, payment terms, and tolerance group.
  - For material master data: Account assignment group, valuation class, and price control.

  Additional fields may be defined locally, above the minimum requirement. (Step 2, 5)
- Customer records must be reviewed annually for activity. Any record with no activity for an extended period (eighteen months) must be deactivated, except for customers under a warranty program. (Step 3)
- Changes to customer and material master data in SAP should only be performed by Service Centers, whenever possible. (Step 4, 6)

Link to: Sanctions and Export Controls Directive and Sanctions and Export Controls Resource Center Intranet

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 AND FREQUENCY

1. Standard prices, discounts, rebates, price changes, and exceptions to standard discounts or rebates must be approved in accordance with the local delegation of authority, reviewed periodically, and properly documented. ***Upon request***
2. The responsible manager must perform a quarterly verification and sign-off to ensure that only authorized users from the Commercial function as defined in the local delegation of authority, or approved Business Service Center users, have access rights to modify pricing data. ***Quarterly***
3. On a quarterly basis, the pricing master data change report, including all pricing condition modifications, must be reviewed and signed off by the responsible manager. Any unauthorized changes identified must be investigated, and appropriate corrective actions must be taken. ***Quarterly***

REQUIREMENTS

- All price determination processes must be defined in a local, written pricing policy that is reviewed and updated regularly (at least every three years). The policy must be formalized in sales contracts or sales orders and comply with legal requirements, as well as fair competition and anti-bribery and corruption laws and regulations. A price list for all products and services must be established by Pricing, Sales, and Marketing, taking into account the various pricing aspects defined in the local pricing policy, including other providers (e.g., transporters, applicators). A complete price list, including effective dates, must be communicated to the responsible team for system update. Backdating of effective prices is not permitted. (Step 1)
- Standard discount and rebate structures must be defined for different customer categories. Each type of discount or rebate must be described in the company's policy with defined objectives and clear application rules, approved by management and validated by local Legal and Compliance. Backdating of discount and rebate schemes is not permitted. (Step 1)
- Exceptions to standard discounts and rebates must be defined in accordance with the company's policy and authorized by the designated approver. (Step 1)
- 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). (Step 1)
- Price changes are performed respecting a local segregation of duties within the Commercial function, properly approved, and 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)
- Pricing master data change report available at each region or country is reviewed. (Step 3)

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

REVENUE

22 Control of customer credit limits

PRIMARY OBJECTIVE

Grant prior authorization for customers exceeding their credit limits

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 AND FREQUENCY

1. Prior to shipment, ensure that an automated or manual check is in place to prevent shipment or delivery to customers exceeding their credit limit (credit block). Any change to a customer's credit limit requires approval in accordance with the local delegation of authority. ***Upon request***
2. Letters of credit, guarantees, or note acceptances issued by banks not included in the Holcim Bank List must be sanction-screened and approved by the Country CFO before the release of goods or services. ***Upon request***

REQUIREMENTS

- A credit line to a single customer (at the legal entity level) has to be approved in accordance with the Group Delegated Authorities. Where a sale is secured by Where a sale is secured by a third-party instrument (e.g., letter of credit, stand-by letter of credit, or first demand bank guarantee), the secured amount may be deducted from the risk exposure only if the instrument is a first-demand security (confirmed letter of credit, stand-by letter of credit, or first demand guarantee) and is issued by a first-class bank approved by Group Treasury. Only in this case will the credit limit or line be submitted for approval based on the net risk exposure after deduction of the secured amount. (Step 1)
- Credit limit checks must be performed for all sales orders. Orders exceeding a customer's credit limit must be managed and approved in accordance with the established procedure and the local delegation of authority. (Step 1)
- No shipments are permitted when a customer exceeds their credit limit until the following conditions are met: (Step 1)
  - The increased credit limit has been properly approved in accordance with the local delegation of authority and updated in the system.
  - The individual order has been released following a documented and effective approval process to avoid unnecessary disruption.
  - All invoices, deliveries, credit notes, and orders have been included in the calculation of the customer balance to compare it against the credit limit.
  - Any practice of bypassing a hold on customer shipments (e.g., manual shipment, fictitious cash customer account) is restricted and tracked through exception reports. Corrective actions must be documented and closed in accordance with the company's policy.
- If applicable, all letters of credit, guarantees, or note acceptances must be issued or confirmed by a bank included in the Holcim Bank List before the release of goods or services. The acceptance of banks not included in the Holcim Bank List is subject to sanctions screening and approval by the Country CFO. (Step 2)

Link to: Group Delegated Authorities, Finance Policy, Sanctions and Export Controls Directive and Holcim Bank List

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 or shipments (Step 1, 2, 4, 5)
- Unauthorized commercial commitments and conditions (Step 1, 2, 3, 4, 5)
- Inaccurate or fraudulent revenue recognition (Step 1, 2, 3, 4, 5)

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL AND FREQUENCY

1. Quantities must be reconciled monthly, and any differences identified in the matching of sales orders, invoices, and shipments, including deviations from weighbridge tolerances, must be corrected to ensure that all deliveries are invoiced. ***Monthly***
2. An annual calibration must be performed for all weighbridges and measurement equipment used for dispatching goods at sites. ***Annual***
3. Unbilled items must be reconciled by the billing team on a weekly basis, or in line with the locally defined invoicing frequency, and any open cases must be resolved within one week. ***Upon change***
4. Finance must verify and approve, on a monthly basis, any sales accruals required at month-end based on unbilled items. ***Monthly***
5. Open sales orders with planned delivery dates in the past that have not been shipped or invoiced must be reviewed monthly and resolved in a timely manner. ***Monthly***

23 Matching of sales orders, shipments and invoices

REQUIREMENTS

- All sales orders, shipments, and invoices must be recorded in the relevant applications. (Step 1)
- Amounts invoiced must be accurate, either verified when manually calculated or automatically calculated by the application system using standard programmed algorithms and established terms of sale, including unit prices, discounts, and rebate rates. (Step 1)
- Invoices and billing data (e.g., quantities, price, discount, rebates, product, customer data) must be matched with sales orders, quantities shipped, and customer master. An automated match must be performed between the invoice and the sales order, including all relevant data. (Step 1)
- Any differences are investigated, and related adjustments are approved and documented (e.g., returns, re-dispatch, intercompany mismatches, or cut-off adjustments). A predefined tolerance threshold is established at the weighbridges for dispatched goods. In addition, discounts and taxes must match the approved parameters in the system, from sales order to invoice. (Step 1)
- Weighbridges and measurement equipment must be recalibrated at least annually, in accordance with local regulations. (Step 2)
- A follow-up on unbilled items must take place at least at month-end. The unbilled items report must be reviewed weekly (or in line with the locally defined invoicing frequency) by the Billing team, and all unbilled items must be invoiced within one week from the date they first appear in the report and within the same reporting month as the delivery. At each month-end, the Sales Manager must receive the report, including documentation of any follow-up actions. (Step 3)
- All orders must be processed in the SAP SD (Sales and Distribution) module, including all discounts and rebates. Direct bookings in the SAP FI (Financial Accounting) module are not allowed. (Step 4)
- Finance must verify and approve any required adjustment entries (e.g., sales accruals) at month-end, based on unbilled items. (Step 4)
- Rules for the closure of open sales orders with delivery dates in the past must be defined locally in accordance with the sales terms and conditions and must be resolved at least semi-annually. (Step 5)

24 Accounts receivable valuation

PRIMARY OBJECTIVE

Ensure that Accounts Receivable balances are reviewed and that provisions are recorded on a quarterly basis

RISK
- Unauthorized or erroneous sales orders 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 AND FREQUENCY

1. A quarterly review and approval of the provision for bad debt must be performed by the designated Finance person. ***Quarterly***
2. The Credit Committee must monitor doubtful Accounts Receivable balances at least quarterly. ***Quarterly***
3. Accounts Receivable write-offs must be recorded only after approval by the Credit Committee, in accordance with the local delegation of authority and the Group Delegated Authorities. ***Upon request***

REQUIREMENTS

- The bad debt provision must reflect the risk of debt recoverability at the end of each reporting period and be assessed quarterly, ensuring the following: (Step 1, 2)
  - Reconciliation of trade balances with the customers must take place, and documentation kept to demonstrate efforts 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 (ECL) model. 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 Receivable, prepaid expenses, and other current assets (IFRS 9).
  - Any change is clearly documented and justified 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 doubtful Accounts Receivable balances.
- A review of specific Accounts Receivable balances indicating uncollectibility must be performed to determine whether they should be written off. Uncollectibility is evidenced by significant financial difficulty of the debtor, a high probability of bankruptcy, or other situations as defined in HARP: (Step 3)
  - Write-offs are determined by the Credit Committee based on appropriate supporting documentation.
  - Write-offs must be approved in accordance with the Group Delegated Authorities and the local delegation of authority.
  - If receivables are collected after being written off, the amounts collected must be credited directly to the company's bank account, and the Accounts Receivable department must be informed accordingly.

Link to: Group Delegated Authorities, Finance Policy and HARP 3.1.1.1.5 Accounts Receivable Trade

PEOPLE

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

PRIMARY OBJECTIVE

Ensure that onboarding, offboarding, and worker transfer processes, including employee master data management, are in place and cover payroll changes, recovery of assets, and system access termination, in compliance with legal requirements

RISK

- Lack or ineffective People 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 AND FREQUENCY

1. Employment contracts or hiring documentation must be signed by both the employee and the company for all employees. This includes the completion of a Compliance Negative Reference Check for Senior Leaders Group, local Executive Committee positions, or external individuals designated as members of the Board of Directors of any Holcim Group entity. ***Upon request***
2. The People team or the business must notify the IT department to request termination of all system accesses before the user's last working day. The People team must also confirm that all company assets have been recovered from terminated employees and that their system accesses were deactivated prior to final payroll payments. ***Upon request***
3. A quarterly verification must be performed by the People team and the cost center responsible person to ensure that the headcount report is accurate (includes only active employees, and reflects proper coding and classification). ***Quarterly***
4. A quarterly review and sign-off must be performed by the control owner for a minimum of twenty-five randomly selected changes to the employee master data to confirm that all changes were based on approved requests and executed by authorized users. ***Quarterly***
5. A monthly validation of employee movements (hire, transfer, promotion, and departure) must be performed to ensure that all changes are accurately recorded in the employee master data and that data is consistent between the local ERP system and SuccessFactors master data. ***Monthly***
6. A quarterly verification and sign-off must be performed by the control owner to ensure that only authorized users from the People department have access to manage employee master data in SuccessFactors and employee data in the local ERP system. ***Quarterly***

REQUIREMENTS

- Employment contracts or hiring documentation must exist for all employees and be signed in accordance with the Group Delegated Authorities or the local delegation of authority. Employment contracts (where required by law) or hiring documentation for all new employees must reference the Code of Ethics and specify that disciplinary measures may be taken on the basis of this document in the event of a breach. (Step 1)
- For all new appointments to a Senior Leaders Group, local Executive Committee positions, or external individuals designated as members of the Board of Directors of any Holcim Group entity, the appointing manager or the People team must request a Compliance Negative Reference Check from the applicable Region Compliance Officer (or delegate), and for Group-level appointments, from Group Compliance. (Step 1)
- A mechanism must be in place to ensure that the People Process administration is informed in a timely manner of all movements of employees and temporary workers paid through payroll, including onboarding, offboarding, and position changes. (Step 2)
- For employees changing positions or leaving the company, a process must be in place to monitor the recovery of all company assets by notifying the relevant departments and obtaining confirmation of recovery. This includes confirmation from the IT department that system access has been deactivated. (Step 2)
- The user termination process must be agreed between the People team or business and the IT department. The People team or business must notify the IT department on or before the user's last working day (e.g., end of contract, resignation, or termination) to request termination of access from all IT systems. Where the termination process is not automated, the IT department must provide timely confirmation that all system accesses have been terminated, within five working days from the requested date. (Step 2)
- All employee departures must follow a written procedure that ensures compliance with all legal requirements (particularly in cases of lay-off) and confirms that all payroll-related payments have been made once all company assets have been retrieved, where applicable in accordance with local labor legislation. (Step 2)
- At least quarterly, the employee headcount is reviewed and validated for accuracy by the People team and the cost center responsible person to ensure that: 1) all own employees on the payroll are actively employed as per their latest contractual status, 2) employment status (e.g., active, on leave, etc.) and employee classification are accurate, and 3) each payee is coded to the correct cost center. Any discrepancies identified must be resolved within thirty days. (Step 3)

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

REQUIREMENTS

People system master data management:

- After go-live in SuccessFactors, an employee master data management process defining roles, responsibilities, and rules for employee data management must be in place and reviewed quarterly to ensure data quality, security, and compliance. All existing employees must have complete and accurate records in SuccessFactors in accordance with the Data Governance Matrix. The hiring process should be updated and automated as much as possible to meet the requirements of this step. (Step 4)
- Adding or modifying a new employee data requires appropriate approval based on an employee change request supported by the necessary documentation. Each entity's People team must identify the mandatory supporting documents in accordance with local regulations. A check must be performed to confirm that all required information is complete and accurate. Changes to employee master data in SuccessFactors must comply with the standard definitions in the Group People Library, and adhere to global and regional procedures throughout the employee lifecycle (e.g., hire, job change, termination, etc.). (Step 4)
- Quarterly, an employee master data change report is generated, listing all creations, modifications, and deletions to ensure that all changes have been duly approved and performed by authorized users. Any exceptions identified are documented and immediately reported to the Group HRIS team for investigation. Corrective actions must be documented, tracked, and all exceptions closed within two weeks. (Step 4)
- At least monthly, the entity's People team must reconcile employee data between SuccessFactors and the local payroll system to ensure data consistency. Employee movements (hire, transfer, promotion, and departure) must be reviewed to confirm that they are recorded accurately in both systems. Any discrepancies identified must be corrected within thirty days. (Step 5)
- Only authorized users from the People department have access to manage employee master data in SuccessFactors and employee data in the local system. (Step 6)

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

Link to: Group Delegated Authorities, Group People Policy, Compliance Negative Reference Check Procedure, Employee Data Governance Guideline, Global People Data Management Guidelines, SuccessFactors Data Governance Matrix, SuccessFactors Critical and Mandatory Fields, Group People Library, MCS 25.5 Data Consistency Manual, MCS 25.6 Manual, SuccessFactors Security Roles, SuccessFactors Security Template, and HARP 6.11.1.01 Personnel [FTE]

26 Payroll

PRIMARY OBJECTIVE

Payroll is reviewed, validated, and reconciled before and after processing each 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 AND FREQUENCY

1. A monthly payroll review and approval must be performed by the Payroll team to confirm data accuracy and reasonableness before processing. ***Monthly***
2. The Payroll team must reconcile total payments to the payroll journal after payroll processing. ***Monthly***
3. The cost center responsible person must review and approve the list of employees charged to their department to confirm accuracy. ***Half year***

REQUIREMENTS

- Approval prior to processing payroll: (Step 1)
  - Balancing routine control: For manual and mass upload imports, the Payroll Manager must perform data accuracy checks (e.g., verify that the total hours worked received from the manager match the total hours recorded in the payroll system, and that the total amount of bonuses received from the local People department match the total amount in the payroll system). In cases where the payroll system is integrated with other systems, the interface must ensure data approval from the source system.
  - When a bonus or any other payout is processed (with or without payroll), a secondary approval must be performed to ensure the accuracy of the payout, both at the individual level and for the total amount to be paid.
  - An analytical review comparing payroll results month-over-month must be performed before the bank transfer to justify any variances. The review must include payroll exception reports to identify unusual amounts (e.g., negative values, zero values, or significant increases between two months).
- Reconciliation after payroll processing: For each payroll, the total payment issued from the Treasury account must be reconciled with the payroll journal to ensure that the amount paid to employees matches the amount calculated by the Payroll department. (Step 2)
- At least every six months (e.g., during salary and bonus reviews, budget, Mid-Term Plan, or forecast cycles), or more frequently where the risk is identified as high, the cost center responsible person must validate that the employee costs charged to their department are accurate (total employee cost). High-risk countries are identified by the Region Chief People Officer in coordination with the Region Internal Control Correspondent. Any discrepancies identified must be resolved within thirty days. (Step 3)

Link to: Group People Policy

27 Compliance with payroll and local labor laws

PRIMARY OBJECTIVE

Ensure that payroll and employment practices comply with local labor laws. Work permits and employment contracts must be in place, verified, and kept up to date at all times

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

IMPACT
- Reputational damages
- Financial losses

CONTROL AND FREQUENCY

1. An annual review and assessment must be performed by the People team covering key payroll processes, employment practices, employee liabilities, and applicable laws to ensure compliance. In cases of non-compliance, Finance, Legal, and Compliance must be notified to assess any potential financial impact, provisions, or disclosure requirements. ***Annual***
2. Employee data in the local system must be timely updated in the event of any change. ***Upon change***
3. A quarterly review, follow-up, and closure of open compliance actions related to local labor laws and regulations must be performed. ***Quarterly***

REQUIREMENTS

- The People department must maintain updated information or a checklist of all applicable local labor laws and regulations. An annual assessment must be performed to ensure compliance. Any identified gaps are reported and followed up with timely corrective actions. In cases of non-compliance with local regulations, a risk analysis is performed and communicated to the Finance, Legal, and Compliance departments to determine the potential need for provisions, disclosures, or corrective actions to achieve compliance. (Step 1)
- Employee data in the local system must be kept up to date. Changes must be promptly recorded in employee files or master data upon notification. (Step 2)
- Actions related to any non-compliance must be recorded and followed up quarterly to ensure timely closure. (Step 3)

Link to: Group People Policy and Minimum Substance Requirements Directive

28 Employee pension and benefit plans

PRIMARY OBJECTIVE

Ensure that employee pension and post-employment benefit plans are established in accordance with Group policies and local labor laws, and that they are accurately calculated and properly recorded

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 AND FREQUENCY

1. Any new plan, amendment, or de-risking project related to existing plans must be communicated by the local entity (Plan Sponsor) to the Group Pension and Benefits Governance team and approved in accordance with the Group Delegated Authorities, following the recommendation of the Group Pension and Benefits Governance team. Annually, the Group Pension and Benefits team updates the list of all pension and post-employment benefit plans and confirms with the Group Pension and Benefits Governance team that they are managed in line with the Group Pension and Benefits Directive. ***Annual***
2. Twice per year, the CFO (or designee) must ensure that pension and post-employment benefit plans are valued within the required timelines and in accordance with the requirements and scope defined in the Group Accounting, Reporting and Consolidation pension instructions. The CFO (or designee) must provide a sign-off of the actuarial results, at least annually, in the Group actuary tool (Risk Analyzer by AON), ensuring that inputs and outputs are accurate and that proper accounting entries are recorded. A reconciliation of actuarial data must be performed by the CFO (or designee), with the support of the local actuary, between the Group actuary tool (Risk Analyzer by AON) and SAP Financial Consolidation. ***Half year***

28 Employee pension and benefit plans

REQUIREMENTS

The Group Pension and Benefits Directive defines the scope, objectives, and rules for managing the plans. The Group Accounting, Reporting, and Consolidation team issues detailed instructions for the reporting of post-employment defined benefit plans. (Step 1, 2)

- The Directive sets the rules for the design of pension plans and other post-employment benefits, which must comply with local regulations and market practices.
- The Directive defines the approval rules to be followed for each activity (e.g., closing or freezing pension plans, de-risking liability management, de-risking investment strategy, employer funding contributions, etc.).
- Reporting for post-employment defined benefit plans must follow the process as per instructions issued by Group Accounting, Reporting, and Consolidation. Actuarial methods and assumptions to be used must be aligned with these instructions.
- Reporting must be updated in the Group actuary tool (Risk Analyzer by AON) in accordance with the instructions for the relevant plans. The local actuary uploads the information related to the benefit plans together with the actuarial report.
- The CFO (or designee) reviews and signs off the results and accounting entries, and ensures appropriate controls over inputs (mainly employee data), outputs (actuarial assumptions and final results), and asset valuation.
- The Group oversees the management of its pension plans through the Group Pension and Benefits Governance team. This interdisciplinary team, comprising specialists from Group Finance, People, and Legal functions, acts as a center of expertise for all matters related to pension and other post-employment benefits, and provides recommendations to Group Management.
- The local entity (Plan Sponsor) must inform the Group Pension and Benefits Governance team of any new plan, amendment, or project affecting existing plans, and request approval in accordance with the Group Delegated Authorities.

Link to: Group Delegated Authorities, Group People Policy, Finance Policy, Pension and Benefits Directive, HARP 4.5.2.5 Post Employment Benefits and Group actuary tool (Risk Analyzer by AON) User Guide

EXPENDITURE

29 Management of supplier master data

PRIMARY OBJECTIVE

Ensure that only authorized personnel can create, modify, or delete financially relevant supplier 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 AND FREQUENCY

1. Changes to supplier master data must be performed by an authorized user and based on approved requests. Quarterly review and sign-off by the responsible manager must be conducted on a minimum of twenty-five randomly selected samples to confirm that changes were based on approved requests and executed by authorized users. ***Quarterly***
2. An annual master data quality review must be implemented to identify and block or deactivate duplicate, inconsistent, and inactive supplier accounts. No exceptions are permitted. ***Annual***
3. A quarterly verification and sign-off must be performed by the responsible manager to ensure that only users from the Master Data Management function have access to change supplier master data. ***Quarterly***

REQUIREMENTS

- A supplier master data management process defining roles, responsibilities, and rules must be in place and reviewed when required. (Step 1, 3)
- All potential new suppliers must go through a single entry point to assess their risk profile and initiate the appropriate qualification process prior to onboarding. (Step 1)
- The onboarding of new suppliers requires the submission of a supplier registration form and the appropriate supporting documentation. The inclusion of bank account details must be supported by these documents. Acceptable supporting documents include a RIB, IBAN, bank letter of confirmation, canceled cheque displaying the supplier's name, or bank statement. A verification process must be performed to ensure that all required information and documentation are complete and accurate. (Step 1)
- A duplicate check must be performed before creating a new record. Duplicate records are not permitted. Each entity must formally define its mandatory and critical fields in SAP or the local ERP system, in line with legal and business requirements. The list must include, at a minimum, the legal name, bank details, incoterms, reconciliation account (general ledger), and control data (Goods Receipt-based invoice verification). Additional fields may be defined locally, beyond the minimum. (Step 1)
- For existing suppliers, any changes to bank account details must be supported by appropriate approvals and relevant supporting documentation, in addition to the supplier's formal request for change. Acceptable supporting documents include a RIB, IBAN, bank letter of confirmation, canceled cheque displaying the supplier's name, or bank statement. New bank details may be updated only after completing a callback process using the registered contact information in the master data. The Master Data Management team must document the call through a follow-up confirmation via email or a recorded call. Alternatively, the callback process may be replaced by direct verification of bank account ownership through bank portals, where this option is available. A verification process must be performed to ensure that all required information and documentation are complete and accurate. (Step 1)
- A quarterly master data change report must be generated covering all creations and modifications to ensure that these transactions were performed by authorized users based on approved requests and supporting documentation. (Step 1)
- If any exceptions are identified, they must be documented and reported immediately for investigation. Corrective actions must be documented and tracked. All exceptions must be closed in a timely manner, as defined locally. (Step 1)
- Supplier records must be reviewed annually for data quality, including checks for duplicates, tax codes, bank account details, mismatches between supplier and bank account countries, and inactive suppliers (more than eighteen months). Records must be deactivated or blocked for payment and purchase, except for suppliers under a warranty program. Suppliers identified through procurement supplier reduction strategies must be deactivated and flagged for deletion. (Step 2)

Link to: Procurement Policy and Sustainable Procurement Directive

30 Supplier qualification and performance evaluation

PRIMARY OBJECTIVE

Ensure working with qualified suppliers by implementing a robust system that includes: supplier screening, supplier qualification, ongoing performance evaluation, and consequence management with non-compliant and underperforming suppliers

RISK

- Ineffective or unethical vendor selection process (incl. TPDD process) (Step 1, 2, 3, 4)
- Transaction with sanctioned parties (Step 1)
- Supply chain disruption (Step 2, 3, 4)

IMPACT

- Compliance
- Reputational damages
- Financial losses
- Fraud

CONTROL AND FREQUENCY

1. Screening of suppliers (active and potential) by Procurement (or designee) must be performed based on criteria required by Procurement, Sustainability, and Compliance to identify sanctioned parties and suppliers with high ESG and compliance risk exposure. The screening must occur prior to entering into a transaction or adding a supplier in the supplier master data, and periodically during the time the business relationship lasts. ***Upon request***
2. Qualification of suppliers with high ESG or compliance risk exposure must be conducted in line with the Third Party Due Diligence Directive and methodologies defined by Group Sustainability (Sustainable Procurement). For suppliers with high ESG exposure whether in or out of the Group Compliance due diligence scope, the qualification process by Sustainable Procurement applies. The qualification must be performed before entering in business relationship (pre-qualification) and at least annually during the business relationship (re-qualification). ***Annual***
3. Supplier performance evaluation is to be conducted at least on an annual basis for suppliers that are critical and strategic to ensure business continuity. ***Annual***
4. Consequence management: Countries must terminate the relationship with suppliers that become sanctioned or are not compliant with laws, regulations or ESG requirements; and have poor performance evaluation or unsolved claims; and refuse to implement corrective actions to address non-compliance, underperformance, or outstanding claim issues. ***Upon change***

REQUIREMENTS

- Supplier selection criteria are defined in the Holcim Code of Ethics for Suppliers. (Step 1)
- Before engaging with suppliers from countries designated as having sanctions risk, obtain a sanctions screen (or exemption) from local or region Compliance or Sanctions Board approval, when required. Sanctioned entities or individuals cannot be added to the vendor master data. There should be an ongoing sanctions screening as defined in the Sanctions and Export Controls Directive: systematically as defined in the Trade Compliance Management tool, and at transaction level considering the defined transactions in scope. For suppliers in scope of the Group Compliance due diligence, the Holcim Integrity Gateway must be used. (Step 1, 2)
- All service providers that interact with public officials on behalf of Holcim, or service providers for armed and unarmed guards, security consulting, executive protection, quick reaction forces, security escort and patrol services, including transportation of explosives and cash, have to be screened compliant with the Third Party Due Diligence Directive before entering into business relationships. Each approved Third Party Due Diligence remains valid for three years, after which it must be renewed. (Step 1, 2)
- Suppliers identified as having high ESG risk exposure, have to be qualified according to the Sustainable Procurement Directive and the Sustainable Procurement Management Standard. (Step 1, 2)
- Commercial (financial health) and technical (goods and services) qualifications are to be defined and coordinated by Category Managers as part ot the sourcing strategy. (Step 2)
- Supplier performance evaluation must be conducted at least for critical and strategic suppliers (countries may define their own priorities based on business continuity risk). Any claims will influence a supplier's overall performance score. Refer to the Procurement Policy and the Kraljic Matrix methodology. (Step 3)
- Category Managers must agree on corrective action plans with suppliers that demonstrate poor qualification, weak performance records, repeated unsolved claims, or ESG-related incidents (refer to 'Incidents' in the Sustainable Procurement Management Standard). (Step 4)
- Non-compliant or underperforming suppliers that refuse to implement corrective actions must be flagged as disqualified (blocked in the ERP system), and their contracts to be terminated, following the risk and consequence management process. (Step 4)

Link to: Code of Ethics for Suppliers, Procurement Policy, Third Party Due Diligence Directive, Sanctions and Export Controls Directive, Sustainable Procurement Directive, Shipping Directive, Workers in the Value Chain Directive, Sustainable Procurement Management Standard, and Sanctions and Export Controls Resource Center Intranet

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

PRIMARY OBJECTIVE

Reconcile purchase orders, receipts and invoices (three-way match), or approve two-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 AND FREQUENCY

1. All purchase requisitions or purchase orders (depending on system design) must be approved in the system by the designated approver, in accordance with the local delegation of authority. ***Upon change***
2. Exceptions identified in the three-way match report must be verified and corrected by the designated responsible function (Business or Procurement) and approved in accordance with the local delegation of authority when exceeding the locally defined threshold. ***Upon change***
3. Any two-way match invoices must be approved by the requisitioner or other designated approver, in accordance with the local delegation of authority, to confirm that the amount, workflow, and receipt of goods or services are correct. ***Upon change***
4. Any vendor direct invoices must be approved in the system by the designated approver, in accordance with the local delegation of authority, to confirm that the amount, workflow, and receipt of goods or services are correct. ***Upon change***

REQUIREMENTS

Purchases using purchase orders: (Step 1, 2, 3)

- Purchasing instruments (purchase requests, purchase orders, framework orders, or contracts) must be approved in accordance with country, region, and Group delegations of authority (involving Legal and Finance departments when required) before entering into any commitment with a supplier. (Step 1)
- Supplier invoices must only be cleared for payment after the system automatically matches the purchase order, receipts, and supplier invoice (three-way match), or the purchase order and approved invoice (two-way match). (Step 1, 2, 3)
- Discrepancies between the invoice, purchase order, and receipt must be formally identified, and the system must block the payment process when the discrepancy exceeds the locally defined threshold. Defined thresholds must be documented and approved in accordance with the local delegation of authority. (Step 2)
- Exception reports (for three-way and two-way match deviations) must be distributed regularly for verification and resolution. Payments can only be made once exceptions are cleared and properly justified. When discrepancies exceed the defined threshold, payment requires approval in accordance with the local delegation of authority. (Step 2, 3)

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

- Vendor direct invoices, i.e., invoices recorded in the SAP FI (Financial Accounting) module, that qualify for payment without a purchase order, must be entered into the system and immediately routed through a workflow for review and approval in accordance with the local delegation of authority. Vendor direct invoices are discouraged and must be kept to a minimum. Once the responsible employee has verified the invoice amount, confirmed that the goods or services have been received, and granted approval, the invoice may be cleared for payment.

Link to: Procurement Policy

32 Payment processing

PRIMARY OBJECTIVE

Ensure that all payments and cash disbursements are approved in accordance with local and Group policies and directives

RISK

- Unauthorized 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 AND FREQUENCY

1. All payments and cash disbursements must be approved, prior to payment, in accordance with the Group Delegated Authorities, the local delegation of authority, and related directives and requirements. ***Upon request***

2. Expenditures related to gifts, hospitality, strategic social investments, sponsorships and donations, entertainment, and travel must be identified through the accounting system. Payments that contradict the requirements of the Gifts, Hospitality, Entertainment and Travel Directive or the Strategic Social Investment, Charitable Sponsorships and Donations Directive must be rejected. ***Upon request***

3. A monthly review and approval of accounts payable subledger accounts and the aging report must be performed by the designated Finance person to identify unusual balances and ensure timely corrective actions. ***Monthly***

REQUIREMENTS

- Payments and cash disbursements are approved, prior to actual payment, in accordance with the Group Treasury Directive, the Group Delegated Authorities, the local delegation of authority, and the applicable requirements of MCS 58. (Step 1)
- Payments related to transactions that did not go through a purchase order process, or to invoices recorded directly in the SAP FI (Financial Accounting) module, must be authorized based on appropriate supporting documentation and in accordance with the local delegation of authority, prior to actual payment. Acceptable supporting documents for manual payment requests include: invoice including IBAN or bank details, agreement or contract including IBAN or bank details, official document from local authorities including IBAN or bank details, and official online registry of bank details or IBAN verifiers (e.g., tax office or company registry). Where applicable, countries must comply with local regulations. Bank details must be authenticated using a trustworthy and independent source of information (i.e., not provided by the requestor) through a two-factor verification process. (Step 1)
- The payment process ensures segregation of duties between: 1) approval of payments (requiring at least two authorized persons to sign the cheque or execute the bank transfer), and 2) accounting (preparation of bank journal entries). Disbursements must be processed by a staff member independent from the receipt or invoice matching process. (Step 1)
- Payments to service providers and suppliers falling under the scope of the Third Party Due Diligence Directive or the Sanctions and Export Controls Directive shall only be made once all applicable requirements of MCS 30 have been duly met. (Step 1)
- Sponsorship and donation payments must be reviewed by Compliance and authorized, in accordance with the local delegation of authority, the Group Delegated Authorities, and the Strategic Social Investment, Charitable Sponsorships and Donations Directive, prior to actual payment. (Step 1)
- All business trips require appropriate authorization and controls, which must be adhered to by both Line Managers and employees. Local travel policies shall include an approval system and process in accordance with the Travel and Events Directive. (Step 1)
- A process must be in place to prevent incorrect payments, such as the use of reports to detect duplicate payments, stamping invoices as paid when payment is issued, or implementing other automated system controls. (Step 1)
- Payments made to providers covering gifts, hospitality, entertainment or travel (whether to a private party or a public official) above the threshold defined by the country or Group must be approved through the Holcim Integrity Gateway and in accordance with the rules defined in the Gifts, Hospitality, Entertainment and Travel Directive. Payments or reimbursements of gifts, hospitality, entertainment or travel made in cash or cash equivalents, such as vouchers or gift cards, are not allowed. (Step 1, 2)
- Country CEOs' expenses must be reviewed and approved by the Area Manager or Region Head (this responsibility may be delegated to the Region Head of Finance). If the approval is not provided directly in the ERP system, the offline (e.g., email) approval must be attached in the local approval system. (Step 2)
- As part of the month-end closing process, the accounts payable subledger is reviewed to identify unusual balances (e.g., aged balances, debit amounts, or incorrect currency rates). Debit balances within the accounts payable subledger are analyzed, and their justification is verified (e.g., credit notes, advance payments). Follow-up actions are documented and monitored during the following month. (Step 3)

Link to: Group Delegated Authorities, Travel and Events Directive, Third Party Due Diligence Directive, Treasury Directive, Strategic Social Investment, Charitable Sponsorships and Donations Directive, Gifts, Hospitality, Entertainment and Travel Directive, Capex Directive and HARP 3.2.1.2.25 Other Cost Center Expenses

33 Accrual for expenditures not invoiced

PRIMARY OBJECTIVE

Ensure that all expenditure accruals are accurately recorded in the financial statements and recognized in the appropriate accounting period

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

IMPACT
- Errors in financials

CONTROL AND FREQUENCY

1. All goods receipts (GR) and service receipts (SR) must be recorded before month-end by the responsible locations. The Purchasing Manager (or designated person) must verify that there are no unrecorded goods or service receipts at month-end for goods and services received as per the purchase orders. ***Monthly***
2. The Goods Receipt and Invoice Receipt (GR/IR) account (or equivalent system account) must be cleared on an ongoing basis and before month-end closing by the designated person from Business or Procurement. ***Monthly***
3. Accruals must be recorded monthly by the Accounting function for all purchases and expenses with pending invoices. Any adjustment to accruals must be approved by the appropriate Finance responsible person. ***Monthly***

REQUIREMENTS

- A process must be in place to review open purchase orders in order to detect unrecorded goods and services received. Open purchase orders with past delivery dates must be monitored, and purchase orders with open quantities that are no longer required must be closed. (Step 1)
- All goods receipts or services rendered that meet all specifications (e.g., quantity, quality), along with the corresponding vendor invoices, must be recorded in the system on a timely basis. If goods or services are received but the invoice is missing, an accrual must be created in the system. The Purchasing Manager reviews the accruals monthly to ensure their reasonableness. (Step 1)
- The SAP GR/IR clearing account serves as an intermediary account for goods and invoices in transit. It represents the Goods Receipt and Invoice Receipt (GR/IR) account, which is a balance sheet account and therefore carries a balance at the end of the period. Differences between goods receipts and invoice receipts must be reconciled by identifying missing corresponding invoices or goods receipts. The GR/IR aging report must also be reviewed regularly to ensure that items are cleared on a timely basis. (Step 2)
- For direct purchases, i.e., invoices recorded in the SAP FI (Financial Accounting) module, the responsible department must inform the Accounting department before month-end of any invoices not yet received or recorded. The Accounting department reviews the missing invoices to determine which expenses should be accrued to ensure proper cut-off. The completeness of accrued services and goods received is validated through a comparison of actual costs to budget, where applicable, and by reviewing open purchase and service orders. Where a full review is not feasible, local thresholds based on budget may be defined. (Step 3)
- Old accrual entries that have not been automatically cleared by the system are followed up monthly and resolved by the Purchasing Manager. Any adjustment related to the current month's accruals is posted by the Accounting department and reviewed by the appropriate Finance responsible person. (Step 3)

Link to: Finance Policy

INVENTORY

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

PRIMARY OBJECTIVE

Ensure the accuracy and completeness of inventory records by performing physical stocktakes of parts and supplies at least annually, and of materials at least monthly, so that recorded descriptions, quantities, and values are correct

RISK

- Inaccurate or fraudulent recording and tracking of inventory (Step 1, 2, 3, 4, 5)
- 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, 5)

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL AND FREQUENCY

1. Physical verification of parts and supplies must be performed annually, or by rotation throughout the year. Count results must be documented, and any discrepancies must be approved and adjusted in accordance with defined requirements. ***Annual***

2. Physical verification of materials must be performed monthly by stock owners using appropriate measuring equipment and methods. Counts must be documented, and any discrepancies must be approved, adjusted, and documented in accordance with defined requirements. Discrepancies exceeding 5% must be investigated and justified. The Finance function must participate in the physical verification process as an observer at least on a half-yearly basis. ***Monthly***

3. An end-of-month production data reconciliation must be performed by the Production Manager (or designee) in accordance with defined requirements. The Finance function must verify the stock reconciliation process performed locally at the plant and, when necessary, apply adjustments to the financial statements in line with the local delegation of authority. ***Monthly***

4. An annual independent full stocktake of materials must be performed by a dedicated and competent team that is not part of the stock ownership, such as a third-party service provider or another function within the company. All differences identified must be approved and adjusted in accordance with defined requirements. ***Annual***

CONTROL AND FREQUENCY

5. A quarterly review of critical production data recorded in TIS for cement sites must be performed by the Finance Controller to ensure data integrity, traceability, and proper authorization of changes. This review must include reports showing modifications to the clinker factor, moisture content of all inbound materials, and any additional critical fields defined locally. All changes to these fields must be performed only by authorized users, in line with the local delegation of authority, and must be supported by approved and documented requests. Each change must be jointly signed off by the Process Manager, Quality Manager, Production Manager, and Plant Manager. Specific checks must confirm that the clinker factor is regularly monitored through inventory control and that any change in its value is properly justified, documented, and jointly signed off by the Process Manager, Production Manager, and Plant Manager. ***Quarterly***

REQUIREMENTS

Regular physical stocktakes of parts, supplies, and materials must be organized by the Operations team with participation from the Finance team and performed in accordance with defined procedures. Any alternative approach resulting from business restrictions or specific circumstances must be agreed in advance and approved by Group Internal Control.

PARTS AND SUPPLIES (Step 1)

Parts and supplies include explosives, consumable materials, wear parts (including refractories), diesel and gasoline, packing materials, and non-capitalized critical and rotating spare parts.

- **Preparation of physical inventory**
  - A plant stocktaking procedure describing the scope, objectives, resources, and timeline must be available and applied.
  - A layout map must define the scope of the stocktake. The inventory count scope must include parts with zero or minimum values (such as obsolete parts written off but still stored at the plant) and off-site inventories, and must exclude consigned stocks for customers and suppliers.

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

REQUIREMENTS

- The stocktake plan must be validated by the Functional Manager and communicated to all relevant stakeholders.
- The movement of parts and supplies (receipts, issues, returns, etc.) must be stopped or controlled during the stocktaking process.
- The date, time, and participants of the stocktake process must be recorded.

• **Stocktake**

- Stocktaking must be carried out under adequate supervision.
- Count sheets used for the stocktake must not display system-recorded quantities (blind count).
- The stocktaking process must identify items that exist but are not recorded, as well as items that are recorded but do not exist (floor-to-listing and listing-to-floor).
- Obsolete items must be identified during the stocktaking process.

• **Frequency**

The stocktake of parts and supplies must be performed at least annually. When a full-scope stocktake of parts and supplies is not conducted at year-end, monthly or quarterly cycle counts must be organized to ensure that all parts and supplies are covered within the annual stocktake process.

• **Roles and responsibilities**

- The Site Manager (or designee) must validate and communicate the stocktake plan to all stakeholders. This role is responsible, in line with the local delegation of authority, for reviewing and approving the stocktake and the proposed adjustments.
- The Functional Manager, depending on the nature of the stock, is responsible for organizing and performing the stocktake. This role must sign off the stocktake results and propose adjustments to the Site Manager in case of physical differences.
- The Finance Controller, or an independent designee when necessary, must ensure the reliability of the work performed, including independent on-site observation as part of the count team. This role is also responsible for the inventory reconciliation together with the Functional Manager and, when necessary, for recording adjustments to the financial statements in accordance with the defined delegation of authority.

• **Follow-up on stocktaking results**

- A double count must be performed for any quantity discrepancy exceeding 5%, calculated per material as specified by the business line.
- The codification, description, and labeling of stocks must be checked and updated if necessary.
- Stocktaking results must be reconciled with ERP inventory ledger data by independent personnel who are not involved in inventory management.
- The reconciliation must be reviewed by the Warehouse Manager and the Finance Controller.
- Following reconciliation and approval, adjustment entries must be recorded in the ERP ledgers.
- Discrepancies must be analyzed to identify root causes and to implement corrective actions.

MATERIALS (Step 2, 4)

Materials include raw materials, fuels, semi-finished, and finished goods.

• **Preparation of physical inventory**

- A plant stocktaking procedure describing the scope, objectives, resources, and timeline must be available and applied.
- A layout map must define the scope of the stocktake, including all off-site stocks.
- The stocktake plan must be validated by the Plant Manager and communicated to all relevant stakeholders.

REQUIREMENTS

- The movement of goods (receipts, issues, returns, etc.) must be stopped or controlled during the stocktaking process.
- The date, time, and participants of the stocktake process must be recorded.
- Calculation formulas used to convert physical measurements such as weight, volume, dimensions, and density into standardized inventory quantities must be defined, documented, and communicated in advance of the stocktake.
- All measured quantities must be reconciled from the time and date of measurement through to the end of the month at 24:00 hours.

• **Stock take**

- Stocktaking must be carried out under adequate supervision.
- Count sheets used for the stocktake must not display system-recorded quantities (blind count).
- The stocktaking process must identify items that exist but are not recorded, as well as items that are recorded but do not exist (floor-to-listing and listing-to-floor).
- Obsolete items must be identified during the stocktaking process.

• **Frequency**

- The stocktake of materials must be performed monthly by the Operations team. At least once per year, the stocktake must be conducted by an independent expert, such as a third-party surveyor or another internal function when appropriate.
- A third-party survey is mandatory when required by local law or when the business faces challenges in ensuring an adequate physical inventory due to limited skills, tools, or internal resources.

• **Roles and responsibilities**

- Operations (stock owner) is responsible for inventory planning and for organizing the stocktake to ensure completeness of all stocktake locations. Operations must also provide the necessary competencies, methodology, and tools for the stocktake team.
- Operations (stock owner) is responsible for measuring bulk density, calorific value, and moisture content at reception and at final usage.
- The Operations team must perform the stocktake and sign the stocktake report. The Production Manager and Quarry Manager, or their designees, are responsible for measuring the physical material stocks and proposing adjustments for production figure differences (physical versus theoretical) in TIS and ERP system.
- Plant Managers and Manufacturing Directors, or Business Line Managers, in line with the local delegation of authority, are responsible for reviewing and approving production and stock adjustment proposals.
- The Finance Controller, or an independent designee when necessary, must ensure the reliability of the work performed. The Finance function must participate in the stock measurement process on a monthly basis (for example, by reviewing results, validating reconciliations, or monitoring procedures). Finance, or an independent designee when necessary, must physically participate on-site as part of the count team at least twice per year. The Finance Controller is overall responsible for ensuring compliance and reliability of the stock reconciliation process performed locally at the plant and, when necessary, for recording adjustments to the financial statements in accordance with the defined delegation of authority.

• **Specific matters**

- **Measurement methods and instruments:** Measurement methods and instruments must be optimized to ensure the reliability and accuracy of measurements.

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

REQUIREMENTS

- **Equipment calibration:** Dosing equipment and weighing devices must be calibrated regularly according to a defined schedule. At least four calibrations per year must be performed for weight feeders in raw and cement mills, as well as for fuel and kiln feed dosing devices. All calibration results must be accurately documented, and records must be maintained for at least one calibration per device following its annual overhaul.
- **Heaps geometry:** Whenever possible, bulk material heaps must be shaped into regular geometric forms. Before stock counts, the Production Manager and Mining Engineer must confirm the geometric shape and zero level of all major heaps.
- **Densities:** The bulk density of all materials, in both loose and compacted forms, must be measured and jointly agreed. Each stockpile, whether loose or compacted, must use the corresponding density. Bulk densities must be verified annually or confirmed as unchanged (for example, when the material source or quality has not changed).
- **Moisture:** Each site must have a defined procedure describing the steps for conducting moisture analysis. Moisture analysis must be performed regularly for all raw material and solid fuel deliveries, with results properly documented and retained.
- **Building Solutions:** For all businesses and sites within the Building Solutions category (excluding the ready-mix concrete sub-segment), where the number of inventory material codes (SKUs) is exceptionally high, materials may be counted through monthly cycle counts. The material codes included in each cycle count must rotate based on a predefined inventory classification methodology formalized in the local procedure. This methodology must prioritize inventory management and control using criteria such as value, demand, and usage. The selected methodology must be justified by the business characteristics, inventory size, and objectives, and reviewed and updated annually. Cycle counts must ensure that all material codes are covered at least once within a one-year cycle. Where the business context allows closer monitoring and tighter control, a stricter and more frequent counting approach must be adopted.
- **Dead stock:** For all bulk materials, the total stock reported in the production data report must include both live stock (automatically movable with permanent equipment) and dead stock (not automatically movable). The value of the dead stock must be jointly agreed by the Production Manager and the Finance Controller.
- **Zero and full stock:** For bulk materials, a physical zero-stock level should be reached at least once per year to perform a consistency check between theoretical and physical stock. When a full- or zero-stock level is reached, any discrepancy between book and physical stock must be adjusted.

• **Monthly stock reconciliation (Step 3)**

- An end-of-month production data reconciliation must be performed by the Production Manager or their designee.
- A stock reconciliation must be performed between the measured stock values of all materials, the products delivered, the materials received, and the production and consumption figures for the current month. Reconciliations must be carried out on a dry basis for semi-finished and finished goods, and on a wet basis for raw materials and fuels.

REQUIREMENTS

- The following parameters must remain fixed and cannot be adjusted: semi-finished and finished goods tonnages (shipments, deliveries, and physical stock measurements), and the total operating hours for each semi-finished and finished goods manufacturing unit during the month.
- All physical material quantities from the stocktake inventory must be cross-checked against stock information in the data systems (TIS and other systems) by independent personnel who are not involved in the material stocktake process.
- Discrepancies between the measured physical stock and the stock information recorded in the ERP system for all physical stocks must be analyzed before any production input adjustments are made. The analysis must first focus on the reliability of the information system, the accuracy of the stocktake, and the output of the manufacturing lines for the month. A double count must be performed for any quantity discrepancy exceeding 5%, calculated per material.
- Discrepancies must be analyzed to identify root causes and to implement corrective and preventive actions. Any discrepancy exceeding 5% for semi-finished and finished goods must be investigated and documented with appropriate justification.
- No adjustments may be made in the data systems (TIS, SAP, or JDE) without the required approvals in accordance with the local delegation of authority. The same users must not be authorized to make adjustments in both the production tools (for example, TIS for cement sites) and the ERP inventory modules (for example, SAP or JDE).

• **Monitoring and control of critical production data in TIS (Step 5)**

- **Changes in TIS over critical fields:** A TIS data change report (i.e., DataCorrLog) must be generated quarterly to capture and review all modifications. The Finance Controller must evaluate this report to verify that all changes were performed by authorized users, in accordance with the local delegation of authority, and based on approved and documented requests. Any exceptions identified must be documented immediately, reported for investigation, and tracked through corrective actions. All exceptions must be resolved within the locally defined timeframe. At a minimum, the following TIS data changes are considered critical and require concurrent sign-off from the Process Manager (for factors), Quality Manager (for moisture), Production Manager, and Plant Manager: 1) raw meal to clinker factor or kiln feed to clinker factor (depending on the cement plant's methodology), and 2) moisture content for all inbound materials (e.g., solid fuels and raw materials). Additional critical fields may be defined locally beyond these minimum requirements.
- **Raw meal to clinker factor / kiln feed to clinker factor determination:** The Finance Controller must perform a quarterly review to ensure that formal evidence exists demonstrating that the raw meal to clinker factor or kiln feed to clinker factor (depending on the plant's adopted methodology) is regularly monitored through inventory control. Any changes to this factor in TIS must be properly justified, formally documented, and jointly signed off by the Process Manager, Production Manager, and Plant Manager.

Link to: Finance Policy, Inventory and Warehouse Management - Cement Industrial Framework Intranet, HARP 3.1.1.1.6 Inventories, Inventory and Warehouse Management - Cement Industrial Framework Intranet and HARP 3.2.1.2.30 Inventory Movements Finished Products

35 Inventory valuation

PRIMARY OBJECTIVE

Inventory must be valued appropriately by identifying and recording provisions for obsolete or slow-moving items

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

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL AND FREQUENCY

1. Inventory costing and valuation must be approved in accordance with the local delegation of authority. ***Quarterly***
2. On a half-yearly basis, as part of the hard close process, provisions for obsolescence, slow-moving items, and write-offs must be approved by the CFO (or designee) in accordance with HARP, the local delegation of authority, and the Group Delegated Authorities. ***Half year***

REQUIREMENTS

- The valuation of each type of inventory must be reviewed for consistency with HARP. Inventory costs shall include purchasing costs, conversion costs, and other costs incurred to bring the inventories to their present location and condition (excluding storage costs). (Step 1)
- Purchased products are valued at the purchase price, net of any price deductions such as trade discounts and rebates. Expenses directly related to the acquisition, including insurance, import duties, transport, and handling costs, are included in the value of the inventory. (Step 1)
- Inventory of own-produced finished and intermediate products is valued at actual cost of goods produced, including depreciation and certain distribution costs (e.g., transport to terminals, warehousing, bagging). Standard costing may be used during the year; however, inventories must be restated to actual cost at year-end. Standard costs must be updated at least once per year, at year-end or during the November hard close. (Step 1)
- Inventory provisions for obsolescence and slow-moving spare parts, as well as write-offs, are estimated in accordance with HARP, based on appropriate supporting documentation and applied consistently from year to year. These provisions and write-offs must be approved in line with the local delegation of authority and the Group Delegated Authorities. (Step 2)
- The review for obsolescence and slow-moving spare parts, as well as related provisions and write-offs, is performed on a half-yearly basis during hard close events. (Step 2)
- Inventories of raw materials and kiln fuels (e.g., coal, petcoke, oil) with no movement for more than three months must be valued at the lower of cost and net realizable value at each site. (Step 2)

Link to: Group Delegated Authorities, Finance Policy, HARP Accounting for Value Adjustment for Different Types of Inventory and HARP 3.1.1.1.6 Inventories

INFORMATION TECHNOLOGY

36 Management of access to IT systems

PRIMARY OBJECTIVE

Access to IT systems is managed 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 AND FREQUENCY

1. Access to IT systems must be granted, modified, or terminated only upon a properly authorized access request, in accordance with the defined procedure. ***Upon request***
2. In the case of terminations, upon receipt of notification from the People department or the business, IT must terminate all user access in a timely manner (within three working days for power users, such as administrators, and within five working days for regular users). ***Upon request***

REQUIREMENTS

Note: IT systems collectively refer to business applications and IT infrastructure, including operating systems, databases, networks, and interfaces.

Granting or changing access: (Step 1)

- A formal user access request form must be completed for every new access or change request to Holcim information systems. The corresponding approver must authorize the request, ensuring compliance with segregation of duties rules.
- The People department must confirm the identity of all internal users and verify the Holcim sponsor for external users.
- External user IDs and temporary Holcim employee accounts must have a defined expiration date of up to twelve months (renewable). Based on the type of ID and associated risks, the sponsor may choose to set a shorter expiration period (e.g., three months). Expiration can be configured at the Google or active directory level where not supported by the application.

Termination: (Step 2)

- This control applies from the moment the People department or the business notifies IT of a user termination request.
- The control over the business notification to IT is defined under MCS 25.
- IT must revoke user access within the defined timelines upon receipt of the termination notification from the People department or the business.

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

37 Review of IT user access rights to production IT systems

PRIMARY OBJECTIVE

IT users must have access rights appropriate to their job role and level of authorization

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

IMPACT
- Operational disruption
- Fraud

CONTROL AND FREQUENCY

1. IT must perform a half-yearly review of all user access rights and permissions for accounts within production systems. ***Half year***
2. Actions such as locking, disabling, or removing user accounts must be taken when access rights are found to be inappropriate. All access changes performed are documented and appropriately retained. ***Upon request***
3. Dormant account reviews must be performed periodically for all IT users (e.g., users not logged in for thirty, sixty, or ninety days), and appropriate actions must be taken. ***Half year***

REQUIREMENTS

Note: IT systems collectively refer to business applications and IT infrastructure, including operating systems, databases, networks, and interfaces.

- This control covers the review of all IT function users (e.g., operating system, database and network administrators, active directory administrators, application support teams, and all other IT users with access to production IT systems). The review of business user access to IT systems is covered under MCS 12 and is therefore out of scope for this control. (Step 1, 2, 3)
- IT users cannot review their own access. The review must confirm that each user's access is consistent with their role and responsibilities. (Step 1)

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

38 Security configuration settings and batch job management

PRIMARY OBJECTIVE

Security configuration settings are reviewed to provide reasonable assurance that unauthorized access to IT systems is prevented. 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 AND FREQUENCY

1. Once a year, the security configuration settings of IT systems must be reviewed to verify that they are appropriate and enforced in accordance with the defined security requirements for applications, operating systems, and databases. Access to identified critical transactions is restricted to users as required. ***Annual***
2. Access to batch job scheduling must be appropriately restricted to authorized users and reviewed on a half-yearly basis. ***Half year***
3. Batch jobs and interfaces must be monitored monthly, and any processing errors must be corrected in a timely manner. ***Monthly***

REQUIREMENTS

Note: IT systems collectively refer to business applications and IT infrastructure, including operating systems, databases, networks, and interfaces.

- Minimum security baseline requirements are defined in the Holcim Minimum Baseline Security Standard and approved by the Group IT Security responsible person. (Step 1)
- The ITSC Security Officer is responsible for obtaining the IT system configuration settings and reviewing them to ensure they comply with, or are stricter than, the defined security configuration baseline. (Step 1)
- For IT systems not managed by Holcim (e.g., cloud-hosted or managed by third parties), the Business or IT function must obtain an independent audit report (e.g., International Standard on Assurance Engagements No. 3402) from the service provider at least annually to verify and follow up on any IT internal control deficiencies identified. (Step 1)
- Critical batch jobs (distinct from end-user-scheduled background jobs) are identified (e.g., interfaces between the ERP system and other critical systems) to ensure that any failures are detected and corrected in a timely manner to maintain data integrity. Access to such scheduled jobs is restricted to authorized users. (Step 2, 3)

Link to: Information Technology Policy, Information Systems User Directive, Artificial Intelligence Directive, Annex 09: IT Controls and Annex 09.01: Holcim Minimum Baseline Security Standard

39 Data backup, storage and restoration process

PRIMARY OBJECTIVE

A data backup, storage, and restoration process is implemented to minimize the risk of data loss

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

IMPACT
- Operational disruption
- Fraud

CONTROL AND FREQUENCY

1. Backups must be performed according to the defined schedule (daily, weekly, monthly, etc.). Backup logs are routinely monitored to verify success and completeness. Any errors identified are reported as incidents and promptly resolved. ***Daily***
2. When external media is used, backups are stored offsite, and media labeling procedures are defined and followed. When online data replication (e.g., storage area network) is implemented, controls must be in place to protect data against corruption and to ensure that corrupted production data is not synchronized in real time to the backup. ***Upon request***
3. Restoration tests must be performed at least annually. Any failures identified are investigated and resolved. ***Annual***

REQUIREMENTS

- The Group IT Infrastructure and Operations Standard defines the IT backup requirements. Local backup and restoration procedures must document the scheduling, backup rotation, retention times, testing of the restoration process, evidence that backups are performed, and evidence of tests performed on the restoration procedure. (Step 1, 2, 3)
- The backup strategy must be designed to minimize the risk of data loss and data corruption (e.g., through controls that prevent backup data corruption). Restoration must be achievable within the business-agreed recovery and restoration time objectives. (Steps 1, 2, 3)

Link to: Information Technology Policy, Information Systems User Directive, Artificial Intelligence Directive, Group IT Infrastructure and Operations Standard and Annex 09: IT Controls

40 Managing changes to IT systems

PRIMARY OBJECTIVE

Prevent unauthorized changes to IT systems

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

IMPACT
- Operational disruption
- Fraud

CONTROL AND FREQUENCY

1. There is a verification to ensure that the requester is authorized to initiate changes to the relevant IT systems. ***Upon request***
2. There is a verification that the requester has followed the defined procedure for requesting changes and that all change requests are approved as required. ***Upon request***
3. A User Acceptance Test must be performed, with additional unit or integration tests conducted if required. The results of the User Acceptance Test must record who performed the test and when it was completed. ***Upon request***
4. There is a verification of the release authorization to ensure evidence is available of who authorized the release and when. ***Upon request***
5. There is a verification that segregation of duties is maintained, ensuring that developers do not move their own changes into the production environment. ***Upon request***
6. There is a verification that test and log evidence exists to support the secure movement of changes into production. Where changes are applied directly in production systems (e.g., configuration or security setting changes), they are reviewed and confirmed for correctness. ***Upon request***

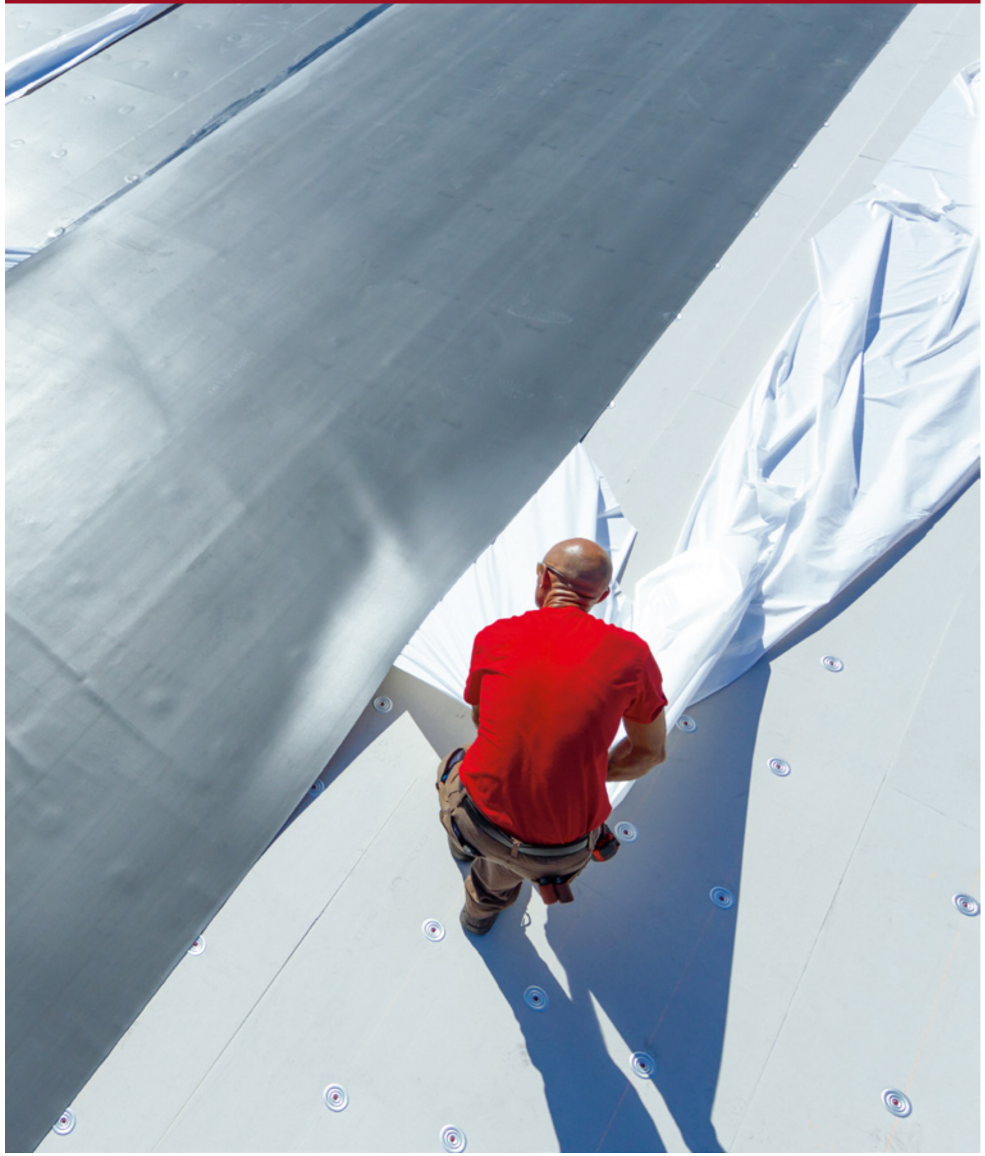
REQUIREMENTS

Note: IT systems collectively refer to business applications and IT infrastructure, including operating systems, databases, networks, and interfaces.

- Changes to IT systems must be requested only by authorized approvers (e.g., application super users or business process owners) to ensure that only valid changes required for business needs are initiated. (Step 1)
- A defined procedure is followed for requesting changes, and all required approvals are captured and recorded. (Step 2)
- The User Acceptance Test must not be performed by the developer or the person responsible for the change, to ensure proper segregation of duties. The User Acceptance Test is performed by application super users or by business- or function-approved testers. (Step 3)
- The Change Approval Board reviews and verifies all changes before granting release approval. Changes must not be moved to production without this approval. (Step 4)
- Developers must not have change access to the production environment. Changes in the production system are moved by administrators (e.g., BASIS for the SAP ERP system). (Step 5)
- Post-change monitoring is performed to ensure that changes are correctly implemented. (Step 6)

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

ACCOUNTING AND CONSOLIDATION



41 Compliance with accounting and reporting standards, and extra-financial data disclosure

PRIMARY OBJECTIVE

Implement and comply with HARP and all applicable regulatory requirements on extra-financial disclosure

RISK
- Non-adherence to accounting, reporting requirements and standards (Step 1, 2)

IMPACT
- Reputational damages
- Errors in financials

CONTROL AND FREQUENCY

1. Confirmation by the CFO of compliance with the Holcim Accounting and Reporting Principles (HARP) and International Financial Reporting Standards (IFRS) is provided through the annual financial certification process. Any deficiencies identified during sustainability reviews conducted by the Group Standards and Accounting Principles (STAP) team are remediated within the agreed timelines. ***Annual***

2. EU Taxonomy-aligned activities and related capital expenditure projects are assessed and documented in the Group EUTA tool and signed off by the CFO (or designee). EU Taxonomy-related financial reporting is performed in accordance with the Group Accounting, Reporting, and Consolidation instructions, under the supervision of the Country EU Taxonomy Finance Coordinator. ***Annual***

REQUIREMENTS

- The Country CFO is responsible for ensuring that HARP requirements are sustained within the company, including updating internal policies to reflect HARP change releases. Adherence to Group standards is confirmed through the annual financial certification process. (Step 1)
- HARP must be implemented in the ERP systems (e.g., SAP, JDE) of all Holcim Group companies. This implementation is certified by the STAP team through a detailed review. (Step 1)
- Each Holcim Group company must have an appointed responsible person for HARP (HARPist). The CFO is responsible for appointing the HARPist, who is an integrated member of the HARPist Virtual Organization, an extension of the STAP team. The appointed HARPist must be recorded in the company list. (Step 1)
- Regular HARP compliance reviews are conducted by the STAP team. Any deficiencies identified must be monitored and remediated by the CFO (or designee). (Step 1)
- The HARP manual includes IFRS elements relevant for Group reporting purposes. Where local circumstances require the application of a specific IFRS not documented in the HARP manual, the Country CFO is responsible for ensuring that the IFRS is properly applied in addition to HARP. (Step 1)
- When a country has a plan to align with the EU Taxonomy, it must include in its Plant Development Plans and Mid-Term Plan the forecasts for aligned sales, as well as action plans to achieve or maintain alignment with the Do No Significant Harm criteria. The country EU Taxonomy Finance Coordinator is appointed and responsible for organizing the assessment of EU Taxonomy-eligible activities in the Group EUTA tool and for ensuring the quality of extra-financial and financial data for EU Taxonomy reporting through capital expenditures (One PPM, where applicable) and financial reporting (in SAP Financial Consolidation). Any inaccuracies or incompleteness identified must be disclosed in the annual financial certification package. (Step 2)

Link to: Finance Policy, HARP Manual, HARP 7.4.4 HARP Sustainability Review and HARP 7.3.7 Taxonomy Reporting

42 Reconciliation of general ledger accounts

PRIMARY OBJECTIVE

Balance sheet accounts are reconciled and reviewed, and the CFO provides sign-off of the trial balance and non-consolidated financial statements

RISK

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

IMPACT

- Errors in financials

CONTROL AND FREQUENCY

1. The CFO (or designee) communicates and monitors the monthly closing checklist. ***Monthly***

2. The CFO (or designee) approves the income statement, balance sheet, and cash flow at least quarterly. ***Quarterly***

3. The designated Finance person approves the subledger-to-general-ledger reconciliations and trial balance on a monthly basis. ***Monthly***

REQUIREMENTS

- The CFO (or designee) prepares, communicates, and monitors a closing checklist (or equivalent schedule document) outlining the key activities to be performed during the close, including task owners and deadlines. (Step 1)
- The CFO (or designee) performs an analytical review of the income statement, balance sheet, and statement of cash flows to identify variances exceeding locally defined thresholds (percentage and amount in local currency) compared to the prior year, and to the forecast or budget. All significant deviations are documented and explained in writing, and any errors are corrected prior to the finalization of the closing. Significant deviations identified during the review are disclosed in writing. Upon completion, 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 prevents manual entries from being posted directly to the general ledger. Any adjustments must be made directly in the subledger. (Step 3)
- The subledger is reconciled to the general ledger on a monthly basis to ensure that the total balance per the subledger agrees with the total balance per the general ledger. Any differences are documented, investigated, and cleared, with all corrections made in the subledger. The reconciliation is reviewed and approved by the designated Finance person. (Step 3)
- For leases under the scope of IFRS 16, lease payments must be reconciled between the SAP RE-FX (Flexible Real Estate Management) module and the local vendor accounting in the ERP system. Right-of-use assets and lease liability accounts must be reconciled with the subledger (detailed by contract) by comparing the fixed asset ledger and the general ledger. (Step 3)
- After all closing journal entries are booked and the subledger-to-general-ledger reconciliations are finalized, a trial balance listing the general ledger balances by account as of the last day of the month is analyzed and reviewed. Any errors identified during the review are corrected before the final closing, and significant deviations are documented and disclosed in writing. Upon completion, the trial balance is reviewed and approved by the designated Finance person. (Step 3)

Link to: Finance Policy and Lease Directive

43 Reconciliation of bank accounts

PRIMARY OBJECTIVE

All bank accounts are reconciled to the general ledger on a regular basis, signed by the CFO, and any required adjustments are recorded immediately

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

IMPACT
- Errors in financials
- Financial losses
- Fraud

CONTROL AND FREQUENCY

1. Monthly bank statements are obtained from the banks, and reconciliations with the general ledger are performed by the responsible Finance person. Required adjusting entries are recorded, and all unreconciled items are followed up and resolved within ninety days. The CFO (or designee) reviews and approves the monthly reconciliation. ***Monthly***

REQUIREMENTS

- Proper segregation of duties is maintained between reconciliation, booking, and approval activities. The person performing the bank reconciliations must not have access to record transactions in the accounting system or to process cash disbursements or receipts. (Step 1)
- All bank statements are reconciled to the general ledger account at least monthly and in a timely manner. Accounts denominated in foreign currencies are revalued at the month-end exchange rate, and the impact is recorded in the general ledger. The bank statement, general ledger balance, and related journal entries are attached to the reconciliation. Reconciling items (differences between book and bank balances) are aged, monitored, and resolved promptly, and any required adjustments to the general ledger are recorded before closing. All bank reconciliations, including those for inactive or dormant accounts, are reviewed and approved by the CFO (or designee) at each month-end closing. (Step 1)
- Local banking regulations governing the clearance of bank transactions must be taken into consideration to ensure timely identification of unreconciled items. (Step 1)
- All reconciling differences must be identified, explained, and, where applicable, formalized with appropriate actions for resolution. Any necessary journal entries to resolve the differences must be posted no later than ninety days after the reconciliation is performed. The bank must be contacted regarding any bank errors, which must also be resolved within ninety days. The use of suspense accounts is not permitted. (Step 1)

Link to: Finance Policy, Treasury Directive and HARP 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 respective partners to ensure the accuracy of the general ledger and proper elimination upon consolidation

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

IMPACT
- Errors in financials
- Financial losses

CONTROL AND FREQUENCY

1. A signed contract must be documented and properly filed for all intercompany transactions. ***Upon request***
2. A monthly review and approval of intercompany and intracompany accounts must be performed by the designated Finance person, including confirmation with each partner or documentation that balances agree in Reco-Live. ***Monthly***
3. All applicable intercompany invoices must be settled through the netting tool within the defined timelines for Group Reporting Units in scope. ***Upon change***

44 Reconciliation of intercompany balances

REQUIREMENTS

- Each intercompany transaction between different legal entities must be supported by a signed contract. Each intercompany invoice must include all relevant details of the goods or services provided, in line with the signed contract. (Step 1)
- All balance sheet and income statement intracompany and intercompany accounts must be formally reconciled with each partner unit in accordance with the criteria defined in HARP, including transactions with other Group companies. Reconciling items must be identified and corrected before the end of the closing. Any foreign exchange difference between the spot rate and the average rate on cash flows with a Group partner must be documented and communicated to Group Accounting, Reporting, and Consolidation before the publication of the consolidated package. Reconciliations must be reviewed and approved by the designated Finance person to ensure that all intercompany balances are fully eliminated upon consolidation. (Step 2)
- Implementation of standardized intercompany settlement process (netting):
  - The netting process and tool (Coprocess) cover the standardized settlement of intercompany invoices. Exceptions are clearly defined in the Netting Scope and Principles, reflecting process limitations and accounting specificities applicable to certain Group Reporting Units. (Step 3)
  - Each Group Reporting Unit must assess its readiness (systems, effort, and efficiency) to integrate into the standardized netting process and update this assessment at least once every three years. The decision to integrate a new Group Reporting Unit into the netting process must be approved by Group Treasury and the process owner. (Step 3)

Link to: Finance Policy, Recharges to Corporate Directive, Netting Scope and Principles, HARP 7.3.3 Reconciliation Policy, HARP 7.3.3.2 Reconciliation Process, HARP 4.11.2 Accounting Treatment for Invoicing of Services within Holcim – other than Industrial Franchise Fee (IFF), and HARP 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 the appropriate personnel

RISK

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

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL AND FREQUENCY

1. All manual journal entries (MJE) must be approved by the designated Finance person in accordance with the local delegation of authority and supported with appropriate documentation prior to posting. ***Upon change***

2. On a quarterly basis, the responsible manager verifies and signs off to ensure that only approved users from the Accounting function have access to post MJE. Each country must also approve, on a quarterly basis, a list of authorized persons who can request MJE from the Business Service Centers. ***Quarterly***

3. The CFO (or designee) performs a monthly verification and sign-off of the analytical review report of posted MJE. ***Monthly***

REQUIREMENTS

MJE are considered high-risk transactions; therefore, they must be kept to a minimum.

Scope: MJE are journal entries posted by a user and not system-generated or automatic entries in the ERP system (e.g., postings from the accounts payable or accounts receivable subledgers). MJE are prepared by individuals to record economic activities outside of subledgers (i.e., directly in the general ledger). When MJE are used, proper review and approval processes must be in place as detailed below.

- Proper segregation of duties is maintained between the MJE requester, approver, and poster. (Step 1)
- MJE must be posted in the system only after they have been reviewed and approved. All MJE require approval prior to posting. Entries relating to valuation adjustments must be approved by the CFO. (Step 1)
- All MJE must include adequate supporting documentation and a clear business rationale, and must be recorded in the correct period and for the correct amount. If the entry is posted by a Business Service Center, the required documentation and information must be provided to them before the posting is released. (Step 1)
- Only users within the Accounting function are authorized to post MJE. (Step 2)
- The CFO (or designee) performs a monthly analytical review of posted MJE, including all required reversals. The review includes statistics on the number, nature, type, and amounts of MJE to detect any unusual activity. Each country defines locally the thresholds and unusual items to be considered in the review. The review must be performed by an individual independent from the person responsible for posting the entries. (Step 3)

Link to: Finance Policy and Annex 14: SAP MJE's Regional Scope

46 Impairment of goodwill, intangible assets and tangible assets

PRIMARY OBJECTIVE

Impairment tests are performed for goodwill, intangible assets, and tangible assets to ensure that their recorded values do not exceed their recoverable amounts

RISK

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

IMPACT

- Errors in financials

CONTROL AND FREQUENCY

1. The Group CFO approves the goodwill impairment test template assumptions, the Mid-Term Plan cash flow data, and any additional data used for the estimate of value in use. (Group level) ***Annual***
2. At least annually, the Country CFO (or designee) approves the impairment tests for intangible assets with indefinite useful lives and for tangible assets. Impairment tests are also performed when a triggering event occurs. Where an impairment is identified, the impairment loss and any related adjustments to the carrying value or useful life (if applicable) are reviewed and approved. ***Annual***
3. The Country CFO (or designee) notifies Group Accounting, Reporting, and Consolidation of any impairment issues as they occur, using the goodwill impairment template. Notifications must also be submitted before the end of May and November each year. ***Half year***

REQUIREMENTS

Cash Generating Unit (CGU): (Step 1)

- The Group's CGU are defined based on the relevant market, typically at a country or product level. For impairment testing purposes, the Group's CGU are aggregated into operating segments, which represent the level reviewed by the Group CEO (the chief operating decision maker). In alignment with IFRS 8, Holcim reports operating segments based on its management structure, following a geographical segmentation. Holcim discloses results under three operating segments: Europe; Latin America; and Asia, Middle East, and Africa. Each segment reports on all product categories, namely Building Materials and Building Solutions.

Goodwill guidance: (Step 1)

- Consequently, all goodwill is tested for impairment by Group Accounting, Reporting, and Consolidation, and not by the Group Reporting Units. The Group goodwill impairment test template is used for this purpose. The cash flows contained in the Mid-Term Plan form the basis of the test, supplemented by any additional required information. The calculations and assumptions must be validated and approved by the Group CFO.

Other intangibles with indefinite useful lives: (Step 2)

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

Property, Plant and Equipment (PPE): (Step 3)

- Group companies must use the impairment template at all times when assessing PPE for impairment.
- All designated assets are assessed at least annually to determine whether any indication of impairment exists. If indicators are identified, a formal estimate of the asset's recoverable amount must be calculated. The review must be documented and formally approved by the appropriate Finance person.
- If an impairment is identified, the impairment loss must be recognized immediately to the extent that the carrying amount exceeds the recoverable amount,
- If there is an indication that an asset may be impaired, the remaining useful life of the asset must be reviewed and adjusted if necessary, even if no impairment loss is recognized.
- Group Accounting, Reporting, and Consolidation must be notified of any impairment issues before the end of May and November each year.

Sustainability: (Step 3)

- An impairment may be required if a tangible asset becomes obsolete, is replaced earlier than expected, or can no longer be used due to newly introduced or more stringent environmental measures.

Link to: Group Delegated Authorities, Finance Policy, Annual ARC Impairment Model and Impairment Testing Guidelines and HARP 4.4.3 Impairment of Assets

47 Transactions in a foreign currency

PRIMARY OBJECTIVE

All transactions in foreign currencies must be identified, recorded, and revalued, and any resulting foreign currency gains or losses must be recognized

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

IMPACT
- Errors in financials

CONTROL AND FREQUENCY

1. The IT Service Centers or the CFO (or designee) approve that the correct Group-communicated exchange rates are entered into the ERP system daily, or at least monthly. ***Monthly***
2. An analytical review of foreign currency gains and losses in the general ledger is performed to ensure that all foreign currency transactions are properly revalued using the month-end rate. ***Monthly***

REQUIREMENTS

- Daily exchange rates published by central banks are typically used to record receivables and liabilities related to foreign currency transactions (settlements and recognized gains or losses). The exchange rate used in the ERP system on the last day of the month is the official rate calculated and defined by the Group and communicated to all countries. Exceptions (i.e., use of daily rates from the central bank on the last day of the month instead of the Group-communicated rate) must be approved by Group Accounting, Reporting, and Consolidation, based on an appropriate impact analysis performed on a half-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 foreign currency transactions, denominated in the transaction currency, so that the ERP system can automatically revalue them until settlement. (Step 2)
- When a transaction is not settled within the same reporting period 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 the transaction is recorded in the system in the foreign currency, the ERP system will perform this revaluation automatically; otherwise, it must be performed manually. (Step 2)

Link to: Finance Policy, Treasury Directive, HARP 3.2.4.4 Foreign Exchange Losses (Gains) and HARP 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 accurate scope of consolidation through proper reporting and disclosure of legal ownership rights

RISK
- Non-adherence to accounting, 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 AND FREQUENCY

1. A new legal entity or any change in the structure of an existing legal entity must be updated in the Legal Entity Management tool (Umbrella) within three days of incorporation or change. The Group Reporting Unit CEO and CFO verify the legal entity structure and sign off on the information in the Legal Entity Management tool (Umbrella) on a half-yearly basis, in accordance with Group Accounting, Reporting, and Consolidation and Group Legal instructions (for the hard closes in May and November each year). ***Half year***
2. The designated Finance person approves the consolidation hierarchy, percentage of ownership, and method of consolidation to ensure correct accounting and reporting treatment, and reconciliation with the Legal Entity Management tool (Umbrella), 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 CEO is responsible for ensuring that all legal entities (without limitation of scope, materiality, or percentage of participation) where direct or indirect control exists, are documented in the Legal Entity Management tool (Umbrella). The CEO and CFO sign off during the May and November hard close events to confirm the completeness and accuracy of the reported information. (Step 1)
- All information in the Legal Entity Management tool (Umbrella) must be updated within three days of any change. (Step 1)
- All information in the Legal Entity Management tool (Umbrella) is mandatory and must be uploaded in accordance with the Legal Entity Management Tool (Umbrella) User Guide. (Step 1)
- A reconciliation for the agreed consolidation hierarchy, between the SAP Financial Consolidation system, and the Legal Entity Management tool (Umbrella) must be performed whenever a change occurs, or at least on a half-yearly basis. (Step 1, 2)
- On a monthly basis, before the start of the country consolidation, the local Reporting team reviews the consolidation hierarchy to verify the completeness and accuracy of the SAP Financial Consolidation set-up, including the legal entities, consolidation methods, and ownership percentages. In case of any changes or uncertainties, alignment with Legal is required, and Group Accounting, Reporting, and Consolidation must be informed accordingly. If the transaction meets the threshold for a Change in Structure (CIS), it must be reflected in the SAP Financial Consolidation package. (Step 2)

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

49 Consolidation of financial statements

PRIMARY OBJECTIVE

The reporting package, including equity and consolidation entries, is reviewed and approved together with the supporting schedules before submission to the Group

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

IMPACT
- Errors in financials

CONTROL AND FREQUENCY

1. The CFO (or designee) reviews and approves the reconciliation between the local equity (general ledger) and the local chart of accounts to the SAP Financial Consolidation reporting package. ***Half year***

2. The CFO (or designee) reviews and signs off on the SAP Financial Consolidation reporting package before submission, in accordance with the defined requirements. ***Monthly***

REQUIREMENTS

- A review is performed to ensure that the amounts reported in the Group reporting package in SAP Financial Consolidation are correct and complete. The mapping between the local chart of accounts and the consolidation package, where applicable, is formalized, and any changes are authorized by the designated Finance person. (Step 1)
- When a country performs a sub-consolidation, the consolidated reporting package is reviewed for completeness and accuracy of the consolidation, where applicable, including: (Step 1)
  - Eliminations, taking into account any non-controlling interest calculations.
  - Accounting for any deconsolidation, acquisition, merger, or transfer.
  - Conversion to the reporting currency and related currency translation adjustments, reviewed for reasonableness using the rates published by the Group and applied in SAP Financial Consolidation.
- A reconciliation between local equity (general ledger) and the Group consolidation accounts in SAP Financial Consolidation is performed twice a year (mid-year and year-end). The reconciliation is approved by the CFO (or designee) and uploaded to the Legal Entity Management tool (Umbrella). All differences are explained, documented, and recorded. (Step 1)
- The country reporting package is reviewed and approved by the appropriate Finance person, the Country CFO, or designee before submission to the Group. The CFO (or designee) formally signs off on the financial statements to confirm that they have been reviewed, that the reported amounts are correct, and that all relevant disclosure information has been included in the appendices. (Step 2)

Link to: Finance Policy, ARC Permanent Instructions and Legal Entity Management Tool (Umbrella) User Guide

50 Statutory financial statements

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials

CONTROL AND FREQUENCY

1. The CFO (or designee) must review and sign off on: 1) the reconciliation between the Group reporting package and the statutory financial statements, including all related adjustments; 2) the statutory financial statements, including the related disclosures; and 3) the reconciliation between the Group reporting package and the statutory financial statements uploaded in the Legal Entity Management tool (Umbrella). ***Annual***
2. Any audit qualifications on the local financial statements must be reported to Group Accounting, Reporting, and Consolidation together with the signed statutory audit reports for the calendar year by April 30 of the following year. Any exceptions must be approved by the Group Head of Accounting, Reporting, and Consolidation before the April 30 deadline. ***Annual***
3. All listed companies must obtain formal approval from the Group Head of Accounting, Reporting, and Consolidation and the Group CFO (or designee) before any external publication of press releases or other reports containing financial information. ***Upon change***

REQUIREMENTS

The negotiation of audit fees, approval of any additional audit-related fees for all Group companies, and the approval of auditor changes at country level are managed in accordance with the Group Delegated Authorities and the Approval of Audit, Audit-Related, and Non-Audit Services Directive.

- A reconciliation between the financial statements in the Group reporting package and the statutory financial statements must be performed to ensure that reported amounts are correct and complete. (Step 1)
- A reconciliation by flow of equity between the Group reporting package and the statutory financial statements must be prepared using the comprehensive template and uploaded to the Legal Entity Management tool (Umbrella) once the statutory financial statements are signed by the auditors. (Step 1)

REQUIREMENTS

- Any adjustments made to the SAP Financial Consolidation reporting package (financial statements) to comply with statutory financial statement regulations (e.g., IFRS to local GAAP) must be documented and approved by the CFO (or designee). (Step 1)
- The CFO (or designee) must formally sign off on the statutory financial statements to confirm that they have been reviewed and that the reported amounts, including all relevant disclosures, are accurate. (Step 1)
- All statutory audits for a given calendar year must be completed by April 30 of the following year. Any exceptions must be approved by the Group Head of Accounting, Reporting, and Consolidation before the April 30 deadline; otherwise, the MCS is considered not adequately implemented. In cases where specific contractual obligations arising from financing transactions or instruments (e.g., bonds, external debt) or other commitments require earlier completion of the financial statements, the applicable contractual deadlines supersede the April 30 timeline for the relevant legal entities. The CFO (or designee) must ensure that the root causes of any delays are analyzed and that corrective actions are implemented to improve the process for the following year. (Step 2)
- For both statutory and Group audits, a mandatory rotation of the audit firm must take place at least every ten years (more frequent intervals may be applied by management). A previously appointed audit firm, after its rotation, cannot be reappointed for a period of at least three years. Additionally, key audit partners must rotate at least every seven years. After rotation, a key audit partner cannot be reappointed, regardless of the audit firm they may subsequently work for. If local regulations in a given country require more frequent rotation or longer waiting periods for reappointment of audit firms or key audit partners, such local regulations supersede this guidance, and the stricter requirements must be applied. (Step 2)
- All listed companies must, at least seven days before the release of the statutory accounts: 1) provide a reconciliation of equity and the main profit and loss indicators to the Group Head of Accounting, Reporting, and Consolidation and the Region CFO. This reconciliation must be reviewed and confirmed by both; and 2) obtain formal approval from the Group Head of Accounting, Reporting, and Consolidation and the Group CFO (or designee) before any external publication of press releases or other externally published reports containing financial information. (Step 3)

Link to: Group Delegated Authorities, Finance Policy, Approval of Audit, Audit-Related and Non-Audit Services Directive, Media Relations Directive, ARC Permanent Instructions, and Legal Entity Management Tool (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 the 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. judgemental assumptions and estimates) (Step 1, 2)

IMPACT
- Errors in financials
- Financial losses

CONTROL AND FREQUENCY

1. A quarterly review and approval must be performed by the Country CFO (or designee) of the provisions reported and the full list of uncertain tax positions at the Group Reporting Unit level, confirming that the reported amounts agree with those in the financial statements. ***Quarterly***

2. A quarterly review and approval of tax risks must be performed at the consolidated Group level by the Group Head of Tax to ensure that all required information is reported, complete, and updated with the latest assumptions. (Group level) ***Quarterly***

REQUIREMENTS

- At least quarterly, the Country CFO (or designee) must track and review the status of all uncertain tax positions, including: (Step 1)
  - The estimated maximum risk and estimated loss.
  - The classification of each position as not probable, probable, or virtually certain.
  - The amount of provisions recorded in the financial statements.
- Based on the quarterly review of uncertain tax positions, adjustments to provisions must be made as required, and related contingencies must be appropriately disclosed. (Step 1)
- The detailed information must be reported to Group Tax using the format and tool defined by Group Tax, with all balances reconciled to SAP Financial Consolidation. (Step 2)

Link to: Group Delegated Authorities, Finance Policy, Tax Reporting Directive, Direct Tax Directive and HARP 7.3.4.04 Tax Risk Reporting

52 Tax filings and payments

PRIMARY OBJECTIVE

Ensure all tax filings and payments are made on time, and that any exceptions are formally 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 AND FREQUENCY

1. The local Tax responsible person and the CFO (or designee) must implement and maintain a tax calendar covering all tax filing and payment due dates. ***Annual***

2. The local Tax responsible person must approve the tax calendar to ensure that all filings and payments are made on time. If an extension is required, approval must be obtained from the Group Head of Tax. ***Annual***

3. Reportable cross-border transactions must be identified and disclosed in a timely manner, in accordance with local requirements. ***Upon request***

REQUIREMENTS

- A tax calendar covering all tax filing and payment due dates must be formally established by the local Tax responsible person and the CFO (or designee). (Step 1)
- A process must be in place to monitor tax filings and payments to ensure they are made on time. All entities must comply with local regulations governing timely filing and payment of tax liabilities. Any request for an extension of filing or payment deadlines must be approved by the Group Head of Tax. (Step 2)
- In accordance with local regulations, reportable cross-border transactions must be identified and disclosed to the tax authorities in a timely manner, where applicable. (Step 3)

Link to: Group Delegated Authorities, Finance Policy, Tax Reporting Directive, EU Mandatory Disclosure Regime (DAC 6) Directive and Direct Tax Directive

53 Deferred and current income tax calculations

PRIMARY OBJECTIVE

Ensure that deferred and income tax calculations are prepared in accordance with Group consolidation instructions, tax policies, directives, and guidance, and comply with local tax regulations

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

IMPACT
- Errors in financials
- Financial losses

CONTROL AND FREQUENCY

1. All income tax and deferred tax calculations, including related documentation, must be reviewed by the local Tax responsible person and approved by the CFO (or designee) at least quarterly. ***Quarterly***

REQUIREMENTS

- A quarterly review of deferred and current income tax calculations, including related documentation, must be performed by the local Tax responsible person and the CFO (or designee). The review includes: (Step 1)
  - Confirmation of appropriate representation on outstanding audits.
  - Verification of compliance with requirements of tax rulings.
  - Assessment of enacted tax rate changes.
  - Review of tax risk provisions and uncertain tax positions, including analysis of changes or expirations, quantification, and probability assessment.
  - Documented analysis of all temporary differences between the tax basis of an asset or liability and its carrying amount per the Statement of Financial Position, including evidence supporting all deferred tax balances.
  - Reconciliation with the amounts booked in the consolidation package.
  - Preparation, documentation, and validation of the tax rate reconciliation.
  - Justification of the recoverability of deferred tax assets through supporting evidence.
  - Verification of account reconciliation ending balances to ensure that all accounts requiring reconciliation are identified and that balances are accurate.

Link to: Group Delegated Authorities, Finance Policy, Tax Reporting Directive, Direct Tax Directive, HARP 3.1.1.2.7 Deferred Tax Assets, HARP 3.1.2.2.3 Deferred Income Taxes and HARP 3.2.6 Income Taxes

54 Transfer pricing

PRIMARY OBJECTIVE

Ensure full compliance with all tax and legal requirements related to intercompany transfer pricing and documentation, with transactions reviewed by Group Tax where required, and any exceptions approved by the Group Head of Tax

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

IMPACT
- Errors in financials
- Financial losses

CONTROL AND FREQUENCY

1. The methodology applied to intercompany transactions must be confirmed by Group Tax and the Region Heads of Tax. (Region and Group level) ***Annual***
2. Any exception to the Group Transfer Pricing Directive must be approved by the Group Head of Tax. (Group level) ***Annual***
3. The local Tax responsible person must review and analyze the entity's transfer pricing practices to ensure compliance with the Group Transfer Pricing Directive. The results of this review must be approved by the CFO (or designee). ***Annual***
4. The local Tax responsible person must maintain and file the transfer pricing documentation, as applicable, in accordance with local requirements and the Group Transfer Pricing Directive. ***Annual***

REQUIREMENTS

- The Transfer Pricing team within Group Tax, together with the Region Heads of Tax, are accountable for analyzing, advising on, and confirming the transfer pricing methodology applied to all intercompany transactions. (Step 1)
- All intercompany transactions must comply with the arm's length principle, as required by local laws and regulations. (Step 1)
- Any exception to the Group Transfer Pricing Directive must be discussed with Group Tax to evaluate the associated risk and formally approved by the Group Head of Tax. (Step 2)
- The entity's transfer pricing practices must be regularly analyzed by the local Tax responsible person and the CFO (or designee) to ensure compliance with the Group Transfer Pricing Directive. The results of the risk analysis must be communicated to the Finance and Legal departments to determine any need for provisions or disclosures, in accordance with MCS 51. (Step 3)
- Transfer pricing documentation must be prepared with the assistance of the Transfer Pricing team within Group Tax and maintained and filed by the local Tax responsible person, in accordance with the Group Transfer Pricing Directive. (Step 4)

Link to: Group Delegated Authorities, Finance Policy, Trading Policy, Direct Tax Directive, Transfer Pricing Directive, Intellectual Property Directive and Recharges to Corporate Directive

55 Non-income (indirect) taxes

PRIMARY OBJECTIVE

Ensure that all non-income tax returns and related account reconciliations are prepared, reviewed, and approved in accordance with local tax requirements and the locally defined frequency

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 AND FREQUENCY

1. All Value Added Tax (VAT) and other indirect tax returns must be reviewed and approved by the CFO (or designee). ***Upon request***
2. The local Tax responsible person must review and approve the reconciliation of current month tax activity, as per the tax calculation, with the corresponding amount in the financial statements. ***Monthly***
3. All Value Added Tax (VAT) accrual and recoverable account reconciliations must be reviewed monthly by the Accounting responsible person and approved by the local Tax responsible person. ***Monthly***
4. The local Tax responsible person must review and approve any unusual activity identified in the Value Added Tax (VAT) reconciliations, including ongoing Value Added Tax (VAT) litigations. ***Monthly***

REQUIREMENTS

- All Value Added Tax (VAT) and other indirect tax returns must be prepared, reviewed, and approved in accordance with local tax requirements and the locally defined frequency. (Step 1)
- The reconciliation between the base used to calculate Value Added Tax (VAT) or sales taxes (e.g., revenue, sales, or other taxable amounts) and the corresponding figures recorded in profit or loss must summarize the current month's sales activity to determine the monthly accrual. Any reconciling items identified must be evaluated to assess their potential impact on the tax return. The reconciliation must reflect information based on the applicable reporting frequency (monthly, quarterly, or annually, depending on the jurisdiction), and any miscellaneous issues (e.g., missed payments, audit findings) must be noted and tracked. (Step 2)
- Reconciliations of Value Added Tax (VAT) accrual and recoverable accounts must be performed by the local Accounting responsible person. Any unusual payments identified during the reconciliation process must be communicated to the local Tax responsible person. (Step 3)
- Value Added Tax (VAT) payments are made from multipurpose cash accounts. Reconciliations of these cash accounts must be performed by the local Accounting responsible person as part of the cash account reconciliation process. Any unusual Value Added Tax (VAT) payments identified during the reconciliation must be reported to the local Tax responsible person. (Step 4)

Link to: Finance Policy

TREASURY

56 Bank relations

PRIMARY OBJECTIVE

Ensure that all bank relationship management activities, including the opening of bank accounts, are conducted and approved by Group Treasury in compliance with the Treasury Directive requirements, and that all signatory guidelines defined in the Treasury Directive are 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 AND FREQUENCY

1. Group Treasury must approve the opening of any bank account, and must be notified when any bank account is closed. ***Upon change***

2. Group Treasury must approve any counterparty not included in the Holcim Bank List before any transactions are initiated. Credit exposure to such counterparties must be continuously monitored to ensure compliance with approved limits. ***Upon request***

3. The local CFO (or designee) must annually approve the list of all bank accounts and the bank account optimization plan, in line with the Treasury Directive. The review must include analysis of inactive accounts and ensure timely closure where applicable. ***Annual***

4. The local CFO (or designee) must quarterly verify that the list of all open bank accounts is reconciled with the Legal Entity Management tool (Umbrella) and the local treasury or accounting system. At least annually, confirmation of authorized signatories must be obtained from banks to ensure alignment with the local delegation of authority. ***Quarterly***

5. Any breaches of approved counterparty risk exposure limits must be reported to Group Treasury, and corrective actions must be implemented within the agreed timeframe. ***Upon change***

REQUIREMENTS

- Bank relationships, including related fees, must be approved in accordance with the Group Delegated Authorities and the Group Treasury Directive, where applicable. (Step 1, 2)
- Bank account openings must receive prior approval from Group Treasury, and closures must be notified to Group Treasury before becoming effective. Each opening or closure must be confirmed by the bank, with evidence retained, and all systems and records, including the Legal Entity Management tool (Umbrella), must be updated accordingly. (Step 1)
- Information provided to banks, including legal and compliance-related matters, must comply with the Group Treasury Directive. (Step 1)
- To limit credit exposure, transactions must only be conducted with authorized counterparties included in the Holcim Bank List, within approved limits and in line with the applicable Group Treasury guidelines. (Step 2)
- Business relationships with banks not included in the Holcim Bank List must receive prior written approval from Group Treasury before any transactions are initiated. Counterparty risk with such non-relationship banks must remain within limits defined through the Group Treasury approval process. The Request for Approval procedure and form must include sanctions screening of the bank, in line with the Group Treasury Directive. (Step 2)
- The local CFO (or designee) must annually review the list of active and inactive bank accounts to ensure that the number of banks and accounts is optimized to enhance cash visibility and reduce risks and costs. The review must identify accounts with no activity for more than six months, and where the setup is not optimized, a plan must be established to close unnecessary accounts within a defined timeframe. (Step 3)
- A reconciliation of the approved bank accounts list with the ERP system and the Legal Entity Management tool (Umbrella) must be performed whenever a change occurs, and at least quarterly. The Legal Entity Management tool (Umbrella) must be kept up to date. (Step 3, 4)
- A process must be in place to: (Step 4)
  - Ensure that only joint signatory rights are granted for any bank transaction, and that each signatory has sufficient seniority to act as an authorized signatory. Authorization limits must be defined for each role in line with the size of the organization.
  - Ensure the immediate removal of signatory rights for employees no longer involved in the payment process, with the bank notified immediately of any signatory changes.
  - Obtain from the banks, at least annually, an updated list of authorized signatories to confirm alignment with the local delegation of authority.
- Cash and deposit limits must be monitored. Any breach of counterparty limits with non-relationship banks must be immediately reported to Group Treasury, and corrective actions must be implemented within the timeframe agreed with Group Treasury. (Step 5)

Link to: Group Delegated Authorities, Finance Policy, Treasury Directive, Sanctions and Export Controls Directive, Minimum Substance Requirements Directive, Holcim Bank List and Legal Entity Management Tool (Umbrella) User Guide

57 Cash transactions are not permitted without Group approval

PRIMARY OBJECTIVE

Cash transactions are not permitted without exceptional approval by the Group

RISK

- Unsecured payment means and 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 AND FREQUENCY

1. If applicable, cash transactions must receive prior approval from Group Treasury and the Group Chief Compliance Officer. The local CFO (or designee) must establish a local procedure with an approval process aligned with Group rules, controls, and thresholds to safeguard and minimize cash and check transactions. ***Upon request***

2. The CFO (or designee) must review and approve the reconciliation of checking and petty cash accounts on a monthly basis. ***Monthly***

REQUIREMENTS

- Cash transactions present a risk of fraud, money laundering, and bribery. Therefore, cash transactions are generally prohibited and may only occur with formal approval from Group Treasury and the Group Chief Compliance Officer. In the absence of such approval, all cash transactions must cease. The following rules must be applied: (Step 1, 2)
  - The maximum allowed petty cash limit per site is CHF 500, without requiring an exception request. Petty cash refers to a small amount of cash kept on site to pay minor expenses (e.g., office supplies or reimbursements) and may include cash withdrawals via corporate credit or debit cards.
  - Supplier payments in cash are not permitted.
  - Cash collections from customers are not accepted.
  - The use of checks is strongly discouraged and should be avoided. If checks are used, only crossed checks (to be deposited into a bank account) are accepted for supplier payments or customer receipts.
  - Cash transactions to buy or sell foreign currencies at banks or exchange offices (bureaux de change) are strictly prohibited. Countries that require such transactions must obtain prior approval from Group Treasury.
  - Cash collections through customer deposits in Cash Deposit Machines (CDM) require prior approval from Group Treasury and Group Compliance.
  - Cash collections and supplier payments via mobile wallets are subject to prior approval from Group Treasury and Group Compliance.
- Any exception to the above requirements must be validated with the Region CFO and approved by Group Treasury and the Group Chief Compliance Officer. The Group CFO must be informed of such approvals. Where exceptions are granted, countries must establish a local procedure to: (Step 1, 2)
  - Safeguard the processes for issuing and collecting cash.
  - Track, record, and support all approved cash and check transactions with appropriate documentation.
  - Maintain segregation of duties between the individual responsible for the physical custody of cash or checkbooks and the bank or cash disbursement authorized signatories. Access to checkbooks, cash, and safes must be restricted to designated persons only.
  - Ensure that an independent person, not responsible for the physical custody of checks, verifies unused checks and reconciles them with the checkbook register on a quarterly basis. Random inventory counts must be performed at least twice per year by an independent person.
  - Reconcile checks and petty cash to the books at least monthly, including petty cash used for employee advances. Any variances must be investigated and approved within the same period before booking.

Link to: Finance Policy and Treasury Directive

58 Secure payment means

PRIMARY OBJECTIVE

Payments are secured to prevent errors and safeguard company assets

RISK

- Unsecured payment means and 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 AND FREQUENCY

1. All users with access to SAP BCM (Bank Communication Manager) sub-module and bank portals must be approved by the CFO (or designee) in line with the local delegation of authority, ensuring dual approval for payments. For Business Service Center users, approval from the Head of the Business Service Center is also required. Access to these systems must be promptly removed upon employee termination or role change. ***Upon request***

2. The CFO (or designee) must quarterly review critical users with payment authorization, payment proposal upload, and administrator access. For Business Service Center users, the review must be performed by the Head of the Business Service Center (or designee). Any inadequate or unjustified dormant access identified during the review must be revoked within three business days. ***Quarterly***

3. The CFO (or designee) must annually review non-critical users with view-only access to bank balances, bank statements, or bank monitor. For Business Service Center users, the review must be performed by the Head of the Business Service Center (or designee). Any inadequate or unjustified dormant access identified during the review must be revoked within five business days. ***Annual***

4. Changes to business partner master data must be performed by an authorized user and supported by an approved request. ***Upon request***

5. The CFO (or designee) must quarterly verify and sign off that only users from authorized functions, with no conflicting roles, have access to change business partner data. ***Quarterly***

6. The Treasurer (or designee) must validate all active direct debits with the relevant banks at least annually. Any direct debit no longer required must be canceled and the bank notified immediately upon identification. ***Annual***

REQUIREMENTS

For bank transfers:

To ensure proper controls are applied, an inventory of all banks must be maintained, including a list of users with access to bank portals and the SAP BCM (Bank Communication Manager) sub-module, managed by the country or Business Service Center. Access to all bank systems, including SAP BCM (Bank Communication Manager) sub-module and bank portals, must be strictly controlled.

- Each user must have a unique user ID and password to access bank portals or the SAP BCM (Bank Communication Manager) sub-module. (Step 1)
- All bank payments must be approved by at least two authorized signatories. (Step 1)
- No modification of system-generated payment data (e.g., supplier bank details, payment amounts, payroll files) is permitted throughout the process. Electronic transfers must be system-coded or encrypted to ensure data integrity and security. Manual upload of payment files into banking platforms is prohibited. (Step 1)
- Banks must systematically provide confirmation that electronic payment files have been received without communication errors, through a positive or negative acknowledgment or an equivalent verification mechanism. (Step 1)
- To minimize fraud risk, Treasurers must reconcile bank and intercompany accounts at a frequency appropriate to the transaction volume and risk (e.g., daily for high-volume operational accounts, weekly for low-volume accounts). Treasurers must not communicate any payment process details to external parties other than banks. (Step 1)
- Manual transfers (e.g., email, letter, or fax requests) must be strictly limited. Upon receiving a manual transfer, the bank must perform a call-back to the Treasurer (or designee) who is independent from the initiator, to reconfirm the transaction before execution. Emails must be marked as confidential, and attachments password-protected. Passwords must be communicated in a separate email. (Step 1)
- Access to the SAP BCM (Bank Communication Manager) sub-module and bank portals must be immediately revoked upon employee termination or role change, in accordance with MCS 36 requirements. (Step 1)
- Critical users: On a quarterly basis, a list of all electronic banking users must be obtained from the bank portals or banks, and users with payment approval access to the SAP BCM (Bank Communication Manager) sub-module must be identified for review. Bank payment authorization access must be restricted to Treasury Operations (Cash and Banking teams). User access to SAP BCM (Bank Communication Manager) sub-module and bank portals must be reviewed against job roles to ensure there is no unauthorized or conflicting access. Users involved in other ERP processes (Master Data Management, Order to Cash, Procure to Pay, or Hire to Retire) must not have payment approval access to bank portals or SAP BCM (Bank Communication Manager) sub-module. Reviewers must not review their own access. (Step 2)
- Non-critical users: On an annual basis, a list of users with view-only access to bank balances, bank statements, or bank monitor must be obtained from the bank portals or banks. A review must be performed to ensure that only authorized users have display access in line with their job roles. Reviewers must not review their own access. (Step 3)
- Dormant users with no activity for over ninety days must be reviewed. Access for users who no longer require it must be revoked within three business days for critical users and within five business days for non-critical users. For all other users, a justification must be documented as part of the review. (Step 2, 3)

58 Secure payment means

REQUIREMENTS

Business partner master data: (Step 4, 5)

- Entities using Treasury Management applications or other payment platforms where business partners (e.g., banks, suppliers, entities) are created and maintained as master data must have a master data management process in place defining roles, responsibilities, and rules, in line with MCS 29 and the related master data management guidelines. The process must ensure that only authorized personnel can create, modify, or delete financially relevant business partner data, supported by the required documentation (e.g., SSI, RIB, IBAN) and bank confirmation where applicable.
- Changes to bank information in Treasury applications or other payment platforms must only occur after completion of a documented callback process using the registered contact details, followed by a confirmation email.

Direct debits: (Step 6)

- The use of direct debit for vendor payments is not permitted unless it is a mandatory requirement imposed by authorities (e.g., tax-related payments). Any exception must be approved by the local CFO and comply with all rules defined in the Treasury Directive.
- The Treasurer (or designee) must ensure that any direct debit payments are executed only in accordance with agreements approved by the CFO.
- An inventory of signed direct debit contracts must be maintained by Treasury, where applicable. The Treasurer (or designee) must confirm this inventory with the relevant banks at least annually.

Link to: Finance Policy and 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, and outstanding positions reconciled with counterparty statements to ensure accuracy and completeness

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL AND FREQUENCY

1. Any new financial instruments, borrowings, commitments, or working capital schemes must be approved in accordance with the local delegation of authority, Group Delegated Authorities, and the Group Treasury Directive. ***Upon request***
2. The CFO (or designee) must review and sign off the list of all outstanding financial instruments, commitments, and working capital schemes. ***Quarterly***
3. For countries trading derivatives locally due to regulatory requirements, the Treasurer (or designee) must review and reconcile outstanding positions with counterparty statements. ***Quarterly***
4. Any cash pool limit increase, including for cash pool participants and all entities in scope, must be approved by Group Treasury. Any cash pool limit breaches must be reported to Group Treasury, and corrective actions must be implemented within the agreed timeframe. ***Upon change***

59 Financial instruments, borrowings, commitments and working capital schemes

REQUIREMENTS

- Financial instruments, borrowings, commitments (e.g., trade finance facilities, surety bonds, guarantee lines), and working capital schemes (e.g., supply chain financing, factoring, off-balance sheet inventory financing) must only be entered into after approval by authorized personnel in accordance with the local delegation of authority, Group Delegated Authorities, and the Group Treasury Directive. The Treasurer (or designee) must maintain a record of all disbursements related to the repayment of borrowings and ensure that both repayments and related borrowings are properly recorded, including the classification of current and non-current portions of liabilities. (Step 1)
- All financing contracts must comply with the Holcim Guide on Loan Documentation. Any exception must be approved by Group Treasury. Financial covenants are not permitted, and any financial contract not aligned with the Holcim Guide on Loan Documentation requires prior approval from Group Treasury. (Step 1, 2)
- The list of all financial instruments, borrowings, commitments, and working capital schemes must be supported by adequate documentation, reviewed and signed off by the CFO (or designee), and reported in accordance with the applicable reporting guidelines. (Step 3)
- Third-party and intercompany financing must be renewed in a timely manner before maturity. (Step 3)
- Countries trading derivatives locally due to regulatory requirements must reconcile counterparty statements with outstanding positions on a quarterly basis. Fair values must align with those provided by Group Treasury. (Step 3)
- Cash pool limits must be approved by Group Treasury, and cash pool drawings must remain within the approved limits. Any potential cash pool limit breach must be immediately reported to Group Treasury, and corrective actions must be implemented within the timeframe agreed with Group Treasury. (Step 4)

Link to: Group Delegated Authorities, Finance Policy, Treasury Directive, Holcim Guide on Loan Documentation, HARP 4.9.2.1 What is a Financial Instrument, HARP 3.1.5 Commitments, Contingencies and Guarantees, HARP 3.1.2.1.13 Supply Chain Financing (SCF), HARP 3.1.1.1.11. Description for Factoring of Trade Receivables reporting (Off / on balance sheet reporting), HARP 3.1.1.1.10 Off-balance Sheet Inventory Financing Arrangement, HARP 3.1.1.1.2 Cash and Cash Equivalents, HARP 3.1.1.1.4 Short-Term Financial Receivables, HARP 3.1.2.1.02 Liabilities From Short-Term Financing, HARP 3.1.1.2.3 Long-Term Financial Receivables, HARP 3.1.2.2.2 Long-Term Financing Liabilities, HARP 4.9.6.1 Credit Lines and Examples for Illustration Purposes, HARP 7.3.4.3.2 Treasury Information Management Column Descriptions, HARP 7.3.4.3.3 Treasury Information Management Row Descriptions and HARP 7.3.4.3.4 Credit Line Column Descriptions

60 Forex, interest rate, commodity risks monitoring and hedging

PRIMARY OBJECTIVE

Exposure to foreign exchange, interest rate, and commodity risks is regularly reported and hedged in accordance 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 AND FREQUENCY

1. The exposure in foreign currencies and any potential foreign exchange or interest rate risks requiring hedging must be reviewed, signed off, and reported monthly to Group Treasury. ***Monthly***
2. The CFO (or designee) must review and approve, on a quarterly basis, the consumption forecast and hedge ratio used to hedge energy price exposure. Any change in the underlying index used to procure the commodity must be communicated to the Energy Front Desk. ***Quarterly***

REQUIREMENTS

- Exposure to foreign exchange and interest rate risks is regularly reported and hedged in accordance with the Group Treasury Directive. (Step 1)
- Foreign exchange risks must be mitigated through natural hedging whenever possible. When natural hedging is not feasible, exposures must be identified and managed in cooperation with Group Treasury, in accordance with the Group Delegated Authorities. (Step 1)
- Speculative activities are strictly prohibited. Country financing and deposit arrangements must be denominated in the functional currency whenever possible. Foreign currency leasing is not permitted. Foreign exchange exposures must be identified and mitigated through natural hedging to the extent possible. (Step 1)
- Exposure to commodity price risk is regularly monitored, hedged, and reported in accordance with the Commodity Price Management Directive for energy. (Step 2)

Link to: Group Delegated Authorities, Finance Policy, Treasury Directive and Commodity Price Management Directive

SUSTAINABILITY

61 Environmental impact

PRIMARY OBJECTIVE

Air emissions, water, and waste are monitored and managed to identify and mitigate 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 water management (e.g. liquid effluents with detrimental impact on water resources) (Step 1)

IMPACT

- Reputational damages
- Operational disruption
- Financial losses

CONTROL AND FREQUENCY

1. Group monitoring and reporting requirements for air emissions, waste, water management, and people must be followed. An annual management review must be conducted to verify compliance with Group policies, directives, and local regulations. Resulting action plans must be documented by the Plant Manager and approved by the Country CEO. ***Annual***

REQUIREMENTS

- All plants must have an environmental management system in place to ensure that environmental impacts and risks are effectively managed and mitigated. Environment-related permits (e.g., general environmental, emissions, water discharge, waste management) must be reviewed annually to ensure compliance. (Step 1)
- All sites must implement the Health, Safety and Environment Critical Controls Management for the Pollution Priority Unwanted Events (PUE), and complete a quarterly verification review in iCare. (Step 1)
- Environmental impacts must be systematically identified through the following steps: (Step 1)
  - Identify environmental aspects of activities, products, and services over which plants have control or influence.
  - Assess the risks associated with the identified environmental aspects that may have a significant impact.
  - Maintain an up-to-date catalog of significant environmental impacts covering both normal and abnormal operations.
- Environmental impacts must be systematically managed to sustain and improve environmental performance while controlling environmental risks across both operations and the supply chain. Progress must be monitored, evaluated, and documented in accordance with local regulations, or at least annually. (Step 1)
- Cement plants must install and operate continuous emission monitoring equipment for dust, nitrogen oxides (NOx), sulfur dioxide (SO_2), volatile organic compounds (VOC), and carbon monoxide (CO), in accordance with the Holcim Emission Monitoring and Reporting Standard. (Step 1)
- Performance improvements in water, circular economy, and people must align with the commitments defined in the Plant Development Plans and other applicable environmental roadmaps. (Step 1)
- Water and waste must be managed with priority given to reuse and recycling over discharge and disposal, in accordance with the Circular Economy Policy, the Health, Safety and Environment (HSE) Internally Generated Waste Standard, and the Health, Safety and Environment Water Management Standard. (Step 1)
- All countries and operating plants must report environmental data and key performance indicators at least annually through the Sustainability Reporting Campaign, in accordance with the Holcim Environmental Reporting Guidelines. (Step 1)
- Group Reporting Units must report sustainability key performance indicators monthly in accordance with Group Accounting, Reporting, and Consolidation instructions. Any inaccuracies or incomplete sustainability key performance indicators in SAP Financial Consolidation must be disclosed in the annual financial certification process. Sustainability indicators reported to the Group must be based on validated data sources and calculation methods, reviewed for reasonableness, and validated by country Sustainable Development senior management on a semi-annual basis. (Step 1)

Link to: Health, Safety and Environmental Policy, Nature Policy, Climate Policy, Circular Economy Policy, Cement Environmental Directive, Water Directive, Quarry Rehabilitation and Biodiversity Directive, Sustainable Procurement Directive, Health, Safety and Environment (HSE) Internally Generated Waste Standard, Health, Safety and Environment Water Management Standard, Holcim Emission Monitoring and Reporting Standards, Holcim Environmental Reporting Guidelines and Health, Safety and Environment Critical Control Management

62 Social impact: human rights and stakeholders

PRIMARY OBJECTIVE

Human rights risks and impacts are identified, addressed, monitored, and remediated across operations, the supply chain, and business partners through the implementation of the Human Rights Approach

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

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

CONTROL AND FREQUENCY

1. Human rights assessments must be performed in accordance with the Human Rights Directive and approved by the entity CEO within the timeframe agreed with Group Sustainability. ***Annual***
2. Human Rights and Stakeholder Engagement Action Plans, including human rights-related grievances, complaints, and follow-up actions, must be reviewed and validated by the local Executive Committee at least annually and signed off by the entity CEO. ***Annual***
3. Human Rights and Stakeholder Engagement Action Plans and related key performance indicators must be submitted by the Group Reporting Units through the Group reporting tool. ***Annual***
4. A Stakeholder Engagement and Human Rights Action Plan must be implemented for all operational sites, supported by a stakeholder mapping that is reviewed and updated annually. ***Annual***
5. Social investments, inclusive business initiatives, and donations must be approved and documented through the Holcim Integrity Gateway in accordance with the Strategic Social Investment, Charitable Sponsorships and Donations Directive, and the Group Delegated Authorities. ***Upon request***

REQUIREMENTS

All Group Reporting Units must ensure that the six elements of the Human Rights Approach are implemented in accordance with the Human Rights and Social Policy and the Human Rights Directive:

- Identify human rights risks and impacts: A Lead designated by the CEO must conduct a human rights assessment at least every three years, based on the entity's risk level, covering operations, suppliers, business partners, and communities. (Step 1)
- Address adverse impacts: All human rights assessments (impact or self-assessments) must result in a Human Rights and Stakeholder Engagement Action Plan that is reviewed at least annually. Major risks or impacts must be immediately included in the Action Plan, addressed by the local Executive Committee, and reported to the relevant Group functions. (Step 1)
- Grievance and remedy: All sites must provide accessible reporting channels for internal and external stakeholders to report human rights-related concerns or grievances linked to operations, in line with the SpeakUp and Investigations Directive and MCS 01. All reported concerns must be registered, and where investigations are conducted locally, the resulting follow-up actions must be incorporated into the Human Rights and Stakeholder Engagement Action Plan. (Step 2)
- Stakeholder engagement: Each site must maintain a Stakeholder Map and a Human Rights and Stakeholder Engagement Action Plan, managed locally and updated at least annually. Group Sustainability must approve the submitted Stakeholder Map and Action Plan according to the defined Group schedule. Cement plants and grinding units must also establish a Community Advisory Panel (CAP). (Step 3)
- Monitor and communicate: Results of human rights assessments, updated implementation status of Action Plans, and other key performance indicators defined by Group Sustainability must be reported annually through the Group reporting system. (Step 4)
- Manage social initiatives: Social initiatives must be managed based on the local context, in line with Group guidelines and the Group Delegated Authorities. (Step 5)

Link to: Group Delegated Authorities, Human Rights and Social Policy, Human Rights Directive, Strategic Social Investment, Charitable Sponsorships and Donations Directive, Sustainable Procurement Directive, Workers in the Value Chain Directive and SpeakUp and Investigations Directive

63 Climate change

PRIMARY OBJECTIVE

Ensure an effective implementation of the decarbonization roadmap including climate change mitigation and adaptation framework, and reporting

RISK

- Stigmatization of the sector (by investors, customers) (Step 1, 2, 3)
- Deviation from CO_2 reduction standards (incl. internal Group targets) (Step 1, 2, 3)

IMPACT

- Reputational damages
- Errors in financials

CONTROL AND FREQUENCY

1. Climate country strategy: The country's climate-related initiatives, decarbonization roadmap, and climate adaptation action plans related to the EU Taxonomy must be documented in the country strategy and Mid-Term Plan process and signed off by the Country CEO. ***Annual***
2. Capital Expenditures Plan: Countries must ensure that decarbonization-related actions, including capital expenditures and operating expenses, are clearly identified, classified, and submitted in the Group systems. ***Annual***
3. Reporting: Countries must report climate-related key performance indicators monthly in accordance with Group Accounting, Reporting, and Consolidation instructions, following validation by the country Chief Sustainability Officer. ***Monthly***

REQUIREMENTS

Strategy: (Step 1)

- Group companies must include details of their short-, medium-, and long-term climate-related strategies in the country strategy and provide details of the decarbonization roadmap (Scope 1 and Scope 2) in the Mid-Term Plan.
- Country targets must align with the Group decarbonization ambition, and the consolidation of all country decarbonization roadmaps must be confirmed to reflect the Group targets.
- For decarbonization projects involving the use, generation, or purchase of carbon credits, the business case prepared by the country Chief Sustainability Officer (or designee) for Carbon Credit Office approval must be validated by the Country CEO.
- Climate adaptation measures must be considered to ensure alignment with the EU Taxonomy 'Do No Significant Harm' (DNSH) criteria on climate change adaptation and must be documented in the iCare tool.

Capital Expenditures Plan: (Step 2)

- Annually, the country Chief Sustainability Officer (or designee) and the Country CFO must ensure that resource allocations, including capital expenditures and operating expenses for climate-related projects or actions, are incorporated into the country's Mid-Term Plan and reconciled with the Plant Development Plans.
- Green Capital Expenditures, as defined in HARP, must be consistently reflected in the capital expenditures reporting within One PPM (where applicable) and in SAP Financial Consolidation.

Reporting: (Step 3)

- The country Chief Sustainability Officer (or designee) must validate the climate-related financial and non-financial indicators reported to the Group on a monthly basis.
- Climate-related indicators reported to the Group must be based on validated data sources and calculation methods, reviewed for accuracy, and validated annually by the country Chief Sustainability Officer (or designee).
- Carbon credit-related key performance indicators must be reported to the Group by the Project Lead and validated by the country Chief Sustainability Officer as part of the annual reporting campaign.
- Any inaccuracy or incompleteness in key performance indicators within SAP Financial Consolidation must be disclosed in the annual financial certification process.

Link to: Nature Policy, Climate Policy, Circular Economy Policy, Quarry Rehabilitation and Biodiversity Directive, Sustainable Procurement Directive, Carbon Credit Directive, Holcim Cement Industrial Framework (Environment and Sustainability), Holcim Environment Questionnaire, Holcim Sustainable Constructions Questionnaire, Scope 3 Standard, HARP 3.1.8.4 Green CAPEX, HARP 6.2.3 Sustainable Development - CO_2 and HARP 7.3.7 Taxonomy Reporting

OPERATIONAL TECHNOLOGY

64 OT security baseline controls for cement plants and grinding stations

PRIMARY OBJECTIVE

The risk of cyberattacks on the OT systems of cement plants and grinding stations is reduced

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

- Reputational damages
- Operational disruption
- Financial Losses
- Fraud

CONTROL AND FREQUENCY

1. OT roles and responsibilities must be defined and assigned at plant, region, and global levels. The designated OT plant responsible person and users must be trained. Cyber incident response processes and procedures must be developed and implemented. ***Annual***
2. Each plant must maintain and review the OT asset inventory on a quarterly basis. Upgrade and replacement plans must be defined in consultation with, and aligned to, the corporate strategy. ***Quarterly***
3. A secure network architecture must be implemented to segregate IT and OT network zones (PCS, Industrial, Lab, and DMZ) using firewalls. Traffic flows between zones must be controlled, and wireless networks must be restricted unless properly hardened and secured. ***Upon change***
4. Access must be granted on a need-to-know basis upon approval by the Plant Manager (or designee). Access rights must be reviewed annually. Remote connections from external networks must not connect directly to the PCS, Industrial, or Lab zones but only through the DMZ or higher-level zones. Technical measures must be implemented to authenticate, authorize, and monitor all remote access sessions. ***Upon request***
5. An annual verification must be performed to confirm that technical measures to prevent malicious code (e.g., anti-malware and anti-virus solutions) are in place. These measures must be deployed on all OT equipment connected to OT networks and implemented in strict accordance with the defined guidance principles. ***Annual***
6. Backup and restore procedures must be defined and documented for each critical OT system, including requirements for offsite storage of backups. ***Upon change***
7. OT equipment must be located in areas that meet physical and environmental security requirements, and compliance must be verified. ***Annual***

REQUIREMENTS

Note: OT systems collectively refers to cement plant's and grinding station's industrial applications and OT infrastructure, including hardware, operating systems, databases, networks, and interfaces.

The detailed stepwise requirements for this MCS are defined in the Minimum Control Standards for Operational Technology (OT) and apply to each defined control. Full compliance with all requirements is mandatory.

- An OT security organization and governance structure must be established. Regular OT security training must be conducted, and a basic cyber incident response plan must be implemented. (Step 1)
- An OT asset inventory and basic lifecycle management process must be established and maintained. (Step 2)
- The OT network must be separated from the IT network using firewalls, and segmentation must be implemented within the OT network. (Step 3)
- A secured logical access environment, including remote access, must be established. (Step 4)
- Basic endpoint protection systems, such as antivirus or EDR, must be installed on all endpoints. (Step 5)
- Backup and restore procedures for critical OT systems must be documented and implemented. (Step 6)
- OT server rooms must comply with secured access and environmental control requirements. (Step 7)

Link to: Minimum Control Standards for Operational Technology (OT)

ACRONYMS

Accounting, Reporting and Consolidation (ARC)

Anti-Bribery and Corruption (ABC)

Aggregates Reserves Management (ARM)

Biodiversity Indicator and Reporting System (BIRS)

Biodiversity Management Plan (BMP)

Board of Directors (BOD)

Business Resilience Team (BRT)

Business Service Centers (BSC)

Capital Expenditures (CAPEX)

Cash Generating Unit (CGU)

Change in Structure (CIS)

Conflict of Interests (COI)

Construction in Progress (CIP)

Country Chief Executive Officer (CCEO)

Chief Sustainability Officer (CSO)

Country Security Representative (CSR)

Data Universal Numbering System (DUNS)

Delegation of authority (DOA)

Direct Debit (DD)

Directors and Officers (D&O)

Do Not Significant Harm (DNSH)

Enterprise Resource Planning (ERP)

Environmental, Social, and Governance (ESG)

Expected Credit Loss Model (ECL)

Foreign Exchange (FOREX or FX)

Generally Accepted Accounting Principles (GAAP)

Group Delegated Authorities (GDA)

General Data Protection Regulation (GDPR)

Group Insurance and Risk Financing (GIRF)

Group Level Material Risks (GLMR)

Group Reporting Unit (GRU)

Group Treasury or Corporate Finance and Treasury (CFT)

Holcim Front-End Reporting Tool (Hive)

Holcim Accounting and Reporting Principles (HARP)

Health, Safety and Environment (HSE)

Health, Safety and Environment Improvement Plan (HSEIP)

Information Technology (IT)

Information Technology Service Centers (ITSC)

International Financial Reporting Standards (IFRS)

Key Performance Indicators (KPI)

Legal Entity Management Tool (Umbrella)

Manual Journal Entries (MJE)

Minimum Control Standards (MCS)

Operating Expenses (OPEX)

Operational Technology (OT)

Group Pension and Benefits Governance Team (PBGT)

Personally Identifiable Information (PII)

Property Damage / Business Interruption (PDBI)

Plant Development Plans (PDP)

Property, Plant and Equipment (PPE)

Power Purchase Agreements (PPA)

Request for Proposal (RFP)

Risk With Zero Conflicts (RWZC)

SAP Bank Communication Manager (SAP-BCM)

SAP Flexible Real Estate Management (RE-FX)

SAP Governance, Risk, and Compliance (GRC)

SAP Financial Consolidation (SAP-FC)

Security Services with Integrity (SSI)

Segregation of Duties (SOD)

Senior Leaders Group (SLG)

Terrorist and Organised Crime (TOC)

Third Party Due Diligence (TPDD)

Trade Compliance Management (TCM)

Uncertain Tax Positions (UTP)

Value Added Tax (VAT)

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

Cover photo:
Wood Wharf, London, UK
In London's historic Canary Wharf, the mixed-use development Wood Wharf is an icon of sustainable construction. It is blazing a trail as one of the first projects in the UK to use Holcim's low-carbon concrete ECOPact with 20% construction demolition materials inside.