

MINIMUM CONTROL STANDARDS - 2025



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 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, Human Resources, Inventory, Expenditure, IT, Accounting and Consolidation, Tax and 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 regional management certify, through signed letters** to the Group, that they are in place and **operating effectively**.

Group Internal Control

MCS SUMMARY AND CONTENTS

MCS		P.
GOVERNANCE AND COMPLIANCE		11
01	Communication and promotion of the Code of Business Conduct and speak-up culture	12
02	Compliance with Fair Competition laws and requirements	14
03	Related party transactions and conflict of interests	15
04	Board of Directors secretarial requirements	17
05	Health, Safety & Environment	18
06	Risk assessment	19
07	Mitigation of business risks - Security	20
08	Mitigation of business risks - Group insurance	22
09	Mitigation of business risks - Business Resilience System	24
10	Mitigation of business risks - Remediation of deficiencies and non-compliance with MCS	26
11	Personal data protection	28
12	Segregation of duties and user access review	30
13	Delegation of authorities and approval workflows	32
14	Litigation disputes	34
15	Review of contracts by Finance	35
FIXED ASSETS		37
16	Management of titles, licenses and permits	38
17	Quarry reserves and provisions for restoration and rehabilitation	40
18	Classification and depreciation of fixed assets	42
19	Physical verification of fixed assets	44
REVENUE		45
20	Management of customer and material master data	46
21	Price management	48
22	Control of customer credit limits	50
23	Matching of sales orders, shipments and invoices	51
24	Accounts receivable valuation	53

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

MCS		P.
HUMAN RESOURCES		55
25	Execution of onboarding, offboarding, master data management and transfers of workers	56
26	Payroll	59
27	Compliance with payroll and local labor laws	60
28	Employee pension and benefit plans	61
EXPENDITURE		63
29	Management of supplier master data	64
30	Supplier qualification and claim management	66
31	Three-way match, two-way match and direct vendor invoices	68
32	Payment processing	70
33	Accruals for expenditures not invoiced	72
INVENTORY		75
34	Physical stock take of parts and supplies and materials, and volume reconciliations	76
35	Inventory valuation	81
IT		83
36	Management of access to IT systems	84
37	Review of IT user access rights to production IT systems	85
38	Security configuration settings and batch job management	86
39	Data backup, storage and restoration process	87
40	Managing changes to IT systems	88

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

MCS		P.
ACCOUNTING AND CONSOLIDATION		91
41	Compliance with accounting and reporting standards, and extra-financial data disclosure	92
42	Reconciliation of general ledger accounts	94
43	Reconciliation of bank accounts	96
44	Reconciliation of intercompany balances	97
45	Manual journal entries	99
46	Impairment of goodwill, intangible assets and tangible assets	100
47	Transactions in a foreign currency	102
48	Management of legal structure and consolidation hierarchy	103
49	Consolidation of financial statements	105
50	Statutory financial statements	106
TAX		109
51	Tax risk assessment and reporting	110
52	Tax filings and payments	111
53	Deferred and current income tax calculations	112
54	Transfer pricing	113
55	Non-income (indirect) taxes	114
TREASURY		115
56	Bank relations	116
57	Cash transactions are not permitted without the Group approval	118
58	Secure payment means	120
59	Financial instruments, borrowings, commitments and working capital schemes	123
60	Forex, interest rate, commodity risks monitoring and hedging	125
SUSTAINABILITY		127
61	Environmental impact	128
62	Social impact: human rights and stakeholders	130
63	Climate change	132
OPERATIONAL TECHNOLOGY		135
64	OT security baseline controls for cement plants and grinding stations	136

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

Governance and compliance



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

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Compliance
- Reputational damages
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. CEO communication of the Code of Business Conduct and integrity line to employees at least annually, performance of training to risky employees according to the training plan, and acknowledgement of the Code of Business Conduct by newly joined employees, maintained by Human Resources (or designee).

Annual

2. Communication of the Supplier Code of Conduct to suppliers and outsourced service providers, must be documented.

Upon change

3. Remediation by management of any confirmed breach.

Upon request

REQUIREMENTS

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

Link to: Code of Business Conduct, Code of Business Conduct for Suppliers, Anti-Bribery and Corruption Policy, Compliance Policy, Human Rights and Social Policy, SpeakUp & Investigations Directive, Sanctions and Export Controls Directive, Human Rights Directive, Third Party Due Diligence Directive, Sustainable Procurement Directive, Responsible Lobbying and Advocacy Directive and Compliance Training Cycle 2025-2026

2 Compliance with Fair Competition laws and requirements

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Compliance
- Reputational damages
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

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

3 Related party transactions and conflict of interests

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Compliance
- Reputational damages
- Financial losses
- Fraud

CONTROL & FREQUENCY

- 1. Monitoring by the appropriate person (see Decisions with Integrity - Conflict of Interest Directive) and the local Compliance Officer of potential conflict of interests situations reported by employees and any resulting actions or requirements, with documentation kept by the local Legal and Compliance department. *Upon request***
- 2. Perform conflict of interests communication annually. *Annual***
- 3. Review and approval by the Legal department before initiating any business deal or arrangement between a Holcim entity and a shareholder or director's company. *Upon request***
- 4. The insiders' list of employees with access to privileged information on Holcim Ltd is elaborated and handled at Group level, by Legal and Compliance. Group Legal and Compliance sends out a quarterly communication. The insiders' list is cross-checked with Hive users list. (Group level) *Quarterly***
- 5. The insiders' list of employees with access to privileged information on a listed Group company is elaborated and handled at country level, by the Legal department or company secretarial department. The country Legal department sends out a quarterly communication. *Quarterly***

3 Related party transactions and conflict of interests

REQUIREMENTS

- For Group privileged information, Group Legal and Compliance lists all employees that have access to that information. For other publicly listed entities, the entity Legal department may also need to list employees in the entity that have access to privileged information. These lists shall be updated on an ongoing basis. As soon as privileged information, such as consolidated financial data and projects data, is available internally, a communication informing insiders of their obligation of not to trade shall be sent out. The updated list and its previous versions as well as the communication are stored by Group Legal and Compliance (or the applicable listed entity). Permissions regarding access to the folder where the lists are stored and secured must be restricted and controlled. (Step 4)
- Group companies having securities listed on a stock exchange shall adopt a binding Insider Dealing and Market Disclosure setting at least equivalent standards and processes designed to ensure compliance by that Group company and its directors and employees of their respective obligations under applicable laws and regulations. (Step 5)

Link to: Compliance Policy, Anti-Bribery and Corruption Policy, Code of Business Conduct, Insider and Management Transaction Directive, Decisions with Integrity - Conflict of Interest Directive and Compliance Training Cycle 2025-2026

4 Board of Directors secretarial requirements

PRIMARY OBJECTIVE

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

.....

RISK

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

IMPACT

- Reputational damages

CONTROL & FREQUENCY

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

REQUIREMENTS

When required by law, an entity that has a Board of Directors must ensure that all corporate secretarial duties are performed and documented in a timely manner in accordance with the local requirements. On behalf of the Board of Directors, the secretary and chairperson must ensure that the Board of Directors and its committees (if applicable) operate according to the provisions of the local corporate laws, company's articles of incorporation, bylaws, charters or other corporate governance regulations. This includes in particular that: (Step 1)

- Key corporate documents and records are maintained in accordance with applicable retention policies (local law and Group regulations).
- Meetings of the Board are held at least as frequently as required by local law.
- Minutes are taken at the meetings, are approved, and are maintained as part of the corporate records.
- Shareholder and Director's registers are kept up-to-date.
- Annual shareholders meeting occurs, if applicable.

- Any other local legal requirements (the defined secretary should specify all the local legal requirements or liaise with the local Legal team to obtain such information and formalize it).
- The Board of Directors chairperson and secretary shall jointly confirm compliance with all applicable corporate legal requirements by signing a compliance confirmation letter as part of the annual internal control certification process. Objective of this control is considered achieved with the following alternative measures: 1) in case the CEO is a member of the Board, a certification letter signed by the CEO in his/her capacity of a Board member and by the secretary; 2) in case the CEO is not a member of the Board, a certification letter signed by the CEO and the secretary, presented in the Board meeting with formalized meeting minutes signed off by the chairperson of the Board.

Link to: Group Delegated Authorities and Minimum Substance Requirements Directive

5 Health, Safety & Environment

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

- 1. Ensure annually the Health, Safety & Environment Policy is correctly applied by verifying the implementation of rewards and recognition, consequence management, Health, Safety & Environment Improvement Plan completion, employees and contractors training plan, Critical Controls and Health, and Safety & Environment key performance indicators. *Annual***

REQUIREMENTS

Country must ensure that the following 4 sections of the Health, Safety and Environment management system are in place and operating with regular reviews: (Step 1)

- Leadership and Engagement: Rewards, Recognition and Consequence Management program is in place.
- Objectives Planning and Management Review: an annual Health, Safety & Environment Improvement Plan (HSEIP) is set up following the Group process. The Health, Safety & Environment Improvement Plan completion is tracked at the country Executive Committee level and the strategic area of Health, Safety & Environment Improvement Plan is tracked in the Group tracking tool.
- Operations and Support Processes: ensure that all employees and contractors are in scope of the training

plan which must meet minimum expectations of classroom and practical per Health, Safety & Environment standards. Countries must implement the Critical Controls Management as defined by the Group.

- Performance Evaluation: Group Health, Safety & Environment audit and annual self-assessment performed at unit level. Process Safety Management and Incident Reporting and Investigation with incidents correctly classified and action plans kept up-to-date with relevant actions. Road key performance indicators (KPIs) should be reviewed.

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

6 Risk assessment

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Compliance
- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

- 1. A risk assessment is performed annually and documented as per the Group Risk management process. Action plans are defined and monitored for all high risks (as a minimum) in accordance with the Group Risk management guidelines. *Annual***
- 2. Country and service center risk assessment reports are 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

- A Risk Lead is appointed in each country to support the local management with the risk assessment process and to monitor mitigation actions. (Step 1)
- A risk assessment is performed and signed off at least annually and identifies risks with the greatest likelihood of occurring and with the highest potential impact as per the current Group Risk assessment methodology (please refer to Group Risk management guidelines). Risks, risk comments (i.e. description), likelihood (initial and residual), impact (initial and residual) and risk treatment have to be documented in the current Group Risk assessment tool. Minutes of the presentation of the risk assessment

to the country ExCo are 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 Group Risk management guidelines. Action plans (title and description), owner and due date have to be documented in the risk management tool. (Step 1)
- Update of the status of actions in the risk management tool is done when the risk assessment is performed as per the Group requirement. (Step 1).

Link to: Finance Policy

7 Mitigation of business risks - Security

PRIMARY OBJECTIVE

Implement security measures and procedures in accordance with the Security and Resilience 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

REQUIREMENTS

Holcim must implement and manage a Security and Resilience (S&R) program, based on the S&R Governance (policy, Security & Resilience Management System (SRMS) and directives). This applies to all companies controlled by Holcim and their projects throughout the entire lifecycle (e.g. Solutions & Products, Holcim Trading, IT Services Centers, Business Services Centers, etc.).

At a minimum, they must perform the following tasks:

- Ecosystem: capture on an annual basis the country ecosystem (people, assets, etc.) in the Holcim Sites Mapping Application (SMA), including evacuation People on Board (POB), where applicable, using the Country Ecosystem report. (Step 1)
- Risks: validate the S&R Threat Assessment from Group and conduct the Risk Assessment at country level on annual basis using the Country Security Risk Assessment. (Step 1)

CONTROL & FREQUENCY

1. **Annual sign off by the country CEO of the Country Ecosystem report, the Country Security Risk Assessment and the Country Security & Resilience Briefing. *Annual***
2. **Ensure minimum implementation requirements of the Security and Resilience Policy, the Security & Resilience Management System (SRMS), and directives are completed by the country. *Upon request***

- Minimum implementation requirements: (Step 2)
 - Structure: CEO must appoint a fit for purpose country Security Representative (CSR). The appropriate S&R structure/organisation must be properly captured. Risk based mandatory trainings and certifications are completed by the required stakeholders and documented.
 - Budget : publish your total FY-1 country security spend and budget for FY-0 in SMA. Confirm with Procurement the spend extracted from SAP is correctly categorized, using the Security Spend - Global dashboard on a quarterly basis. Ensure correct allocation with one of the three Product and Services Classification System (PSCS).
 - Mitigation controls: implement mitigation controls at the location of the risk and deploy specific plans and/or programs where Group level material risks (GLMRs) and directives (i.e. SSI, TOC) have been identified as 'in-scope'.

REQUIREMENTS

- Travel: Country Travel and Events rules are in place, mirroring the Travel and Events Policy. Appoint a country Travel Coordinator; travel agency(ies) are connected to I-SOS Travel Tracker; the Travel dashboard weekly extract is systematically used to verify visibility of all international business travellers in the Travel Tracker, and that they have completed the mandatory general Business Travel eLearnings and downloaded the Int-SOS mobile application. The country Travel Guide is updated annually.
- Third parties: engage, manage and evaluate suppliers providing security services annually in line with Holcim governance: TPDD (except security equipment suppliers), contract aligned with SSI requirements, purchase orders, and annual evaluation of all manned-guarding private security providers.
- Incident response: report all security incidents through Holcim Security Incident Notification tool (SINT).

Provide evidence that all recurring incidents and High and Very High impact incidents are addressed, lessons learned are captured and mitigation action implemented.

- Audit, Assurance and Performance: (Step 1, 2)
 - track the implementation of the Security & Resilience Management System and the deployment of security directives using the 8 pack tool, and
 - send the Country Security & Resilience Briefing and the Country Ecosystem Report to country CEO and Group Security & Resilience at least annually.

Link to: Security and Resilience Policy, People Security Directive, Security Services with Integrity (SSI) Directive, Terrorist & Organised Crime (TOC) Monitoring Program Directive, Travel and Events Policy, Holcim Business Travel eLearnings, Security & Resilience Management System (SRMS) and SSI Quick Checklist

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

8 Mitigation of business risks - Group insurance

PRIMARY OBJECTIVE

Follow the Group insurance process to ensure adequate risk coverage

RISK

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

IMPACT

- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

The country must comply with the following 5 priorities:

- Group insurance premiums are paid by the due date with no delay. (Step 1)
- Property insurance values are provided annually to Group Insurance and Risk Financing (GIRF) before the due date to avoid under-insurance. (Step 2)
- All claims and losses that are covered by a Group Insurance policy and that are likely to exceed the applicable deductible or exceed EUR 500.000 (or equivalent) have been timely declared to Group Insurance and Risk Financing (GIRF) within 48 hours of incident via the Group Risk Insurance tool (GRIT). (Step 3)
- All Risk Improvement Actions (RIA) recommended by our insurer have to be mitigated within a reasonable timeframe. If Group countries do not agree with the RIA, GIRF must be notified and alternative measures must be put in place. (Step 4)
- Any change in the business that impacts the Group Insurance programs* are communicated to Group Insurance and

Risk Financing (GIRF) (e.g. new business activity like installation of building materials, new products with different liability risks such as building material chemicals, etc.). (Step 4)

- All CapEx projects in excess of EUR 5 million (or equivalent) are reported to Group Insurance and Risk Financing (GIRF) to ensure appropriate coverage. (Step 4)
- For risks that are not covered by Group insurance programs*: (Step 5)
 - local Executive Committee must put in place local insurances as required by local regulations (e.g. motor liability, workers compensation insurance), and
 - local Executive Committee may put in place local insurance for non-mandatory local risks as long as these do not overlap Group insurance programs (e.g. allowed would be fiduciary insurance for local pension fund, trade credit insurance).

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

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

9 Mitigation of business risks - Business Resilience System

PRIMARY OBJECTIVE

Every country must have a Business Resilience program

RISK

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

IMPACT

- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

1. **Annually verify that the following requirements are in place at country level in accordance with the Holcim Business Resilience Directive: *Annual***
 - **appointed Business Resilience sponsor, Business Resilience coordinator and Business Resilience team.**
 - **up to date Country Business Resilience Plan ('Plan on a Page').**
 - **up to date Crisis Management Plan and Business Continuity Plan at country level, Emergency Response Plan available at the location of the risk(s).**
 - **specific country level plans for Group level Material Risks, High and Very High inherent risks, incidents or programs.**
 - **post-exercise reports which include objectives, the risk being exercised and the lessons learnt.**
 - **all recurring incidents and High and Very High incidents are addressed, lessons learnt are captured, and mitigation actions implemented.**

REQUIREMENTS

Holcim must implement and manage a Business Resilience (BR) program, following their Security and Resilience Management System (SRMS) and the Business Resilience Directive requirements. This applies to all companies controlled by Holcim and their projects throughout the entire lifecycle (e.g. Solutions & Products, Holcim Trading, IT Services Centers, Business Services Centers, etc.). In case of a joint Business Resilience program with a Holcim country, a formal agreement should exist.

At a minimum, they must perform the following tasks:

- nominate a Business Resilience sponsor and a coordinator to implement the Business Resilience program. Appoint a Business Resilience team (BRT) consisting at a minimum of a Business Resilience team leader and core members,
- perform and document the training of Business Resilience sponsor, coordinator and Business Resilience team,

- prepare and maintain a Country Business Resilience Plan ('Plan on a Page'),
- maintain and exercise the country level plans for in-scope Group level Material Risks (GLMRs), High and Very High inherent risks identified in the Holcim S&R Risk Assessment tool, within a three-year cycle, or if any changes in personnel or risk,
- perform an annual Business Resilience team exercise of their choice, and
- incident response: report all S&R incidents through the Holcim Security Incident Notification tool (SINT). Provide evidence that all recurring incidents, and High and Very High impact incidents are addressed, lessons learnt are captured, and mitigation actions implemented.

Link to: Security and Resilience Policy, Business Resilience (BR) Directive, People Security Directive and Travel and Events Policy

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

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

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

CONTROL & FREQUENCY

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

REQUIREMENTS

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

- the MCS exception approval process: in case a country is not able to design a local control description in compliance with the Minimum Control Standards requirements, ('Requirements' + 'Control Description'), the country Internal Control Manager clears with regional Internal Control correspondent, uses the MCS Design and Implementation non-compliance approval form to seek Group approval. Submission must be done two weeks prior to the Control Design Assessment (CDA) deadlines. Approvals are to be uploaded/linked at SAP Governance, Risk, and Compliance tool (SAP-GRC), (Step 1)
 - controls rated as 'Not Applicable' and split of responsibility among entities and service centers must be formally validated by regional Internal Control correspondent, (Step 1)
 - deficiencies to Minimum Control Standards have to be validated by local management, region Head (for countries) / Group management (for functions) through the certification process, (Step1)
 - any deficiency related to MCS classified with an impact over compliance:
- MCS 01, 02, 03, 06, 10, 11, 16, 20, 22, 25, 29, 30, 32, 56, 57, 62. (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 before signature of the country Certification Package, (Step 1)
- perform root cause analysis, a detailed description of the deficiency and the creation of an action plan to remediate the weakness identified, (Step 2)
 - deficiencies are communicated to those parties responsible for taking corrective action, at senior management, (Step 2)
 - follow-up of corrective actions and progress towards completion, (Step 2)
 - action plans relating to deficiencies are tracked regularly by the local Executive Committee and to Group Internal Control at least twice a year, and (Step 2)
 - all deficiencies and action plans are tracked in SAP Governance, Risk, and Compliance tool (SAP-GRC). (Step 2)
- Link to: Finance Policy, MCS Design and Implementation non-compliance approval form, Internal Control Instructions and Holcim Financial Certification Permanent Instructions**

11 Personal data protection

PRIMARY OBJECTIVE

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

RISK

- Unauthorized use of company 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 & FREQUENCY

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

REQUIREMENTS

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

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

Link to: Compliance Policy, General Data Protection Directive 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 & FREQUENCY

- 1. Information Technology Service Centers annually review and validate the segregation of duties rules set for enterprise resource planning (ERP) systems and other in-scope applications per region, and provide the confirmation to the countries/functions/service centers. *Annual***
- 2. Review half yearly, at a minimum, of the segregation of duties reports for the enterprise resource planning (ERP) system and other in-scope applications per region, by the respective business process owners and the CFO. Segregation of duties conflicts are removed or mitigated as per the Group requirements. *Half year***
- 3. Validation half yearly, at a minimum, over users' level of access for all critical business applications, including TIS. Any corrective actions are taken within one month after the review, if needed. *Half year***
- 4. Validation half yearly, at a minimum, over dormant users access deletion/revoked. Any corrective actions are taken within one month after the review, if needed. *Half year***

REQUIREMENTS

Segregation of Duties (SoD):

- Information Technology Service Centers (ITSCs) annually review the SoD rule set for enterprise resource planning (ERP) system and other regionally scoped applications for SoD, to ensure alignment with Group rules and update the local customized objects (transactions) with support from business and provides the confirmation to the countries/functions/service centers. Where the SoD ruleset is managed directly by the countries, this should be performed at the country level, (Step 1)
- risks with zero conflicts (RWZC) are eliminated upon identification. There is no tolerance for conflicts over risks mapped as 'risk with zero conflicts', (Step 2)
- other SoD risks (non RWZC) are to be kept at a minimum. Whenever removal is not possible, they are mitigated by implementing a compensating control. These compensating actions must be documented and monitored to ensure they are reducing the identified risk. The compensating controls must be tested for operating effectiveness, (Step 2)
- exceptions of the above, risk with zero conflicts and non-risk with zero conflicts requirements, have to be reviewed and agreed with 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* including TIS:

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

Link to: Finance Policy, Annex 10: Holcim SoD conflicts (RWZC), Annex 10.02: Holcim SAP SoD Rule Set, Annex 09: IT Controls and Annex 09.02: TIS Roles and Security management

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

13 Delegation of authorities and approval workflows

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

Group Delegated Authorities (GDA):

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

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

- an authorization policy or delegation of authority (DoA) matrix must exist to establish clear lines of authority for the approval of all main transactions within monetary limits and other authorizations in the country, such as the signing authorities. As monetary thresholds increase, additional approvals from senior levels of management are required, with the highest monetary thresholds requiring Board of Directors and Executive Committee's approval. This delegation of authority is formally documented, kept up-to-date and signed off by the local Executive Committee, and Board of Directors (when applicable),
- Group Delegated Authorities must be respected within the country delegation of authority matrix. Country authorities and thresholds defined in the Group Delegated Authorities may be delegated locally but such must be documented in the local DoA and approved by the local Executive Committee (and Board of Directors, if applicable),

- responsibilities are clearly stated and communicated within the organization,
- the assignment of responsibilities is clear, including third-party service providers (who carry out activities on behalf of the organization), related to the extent of their decision-making rights,
- the delegation of authority is adhered to for every transaction which requires approval, and
- the delegation of authority matrix is reviewed at least yearly for compliance with the authorization policy or limits definitions and updated as needed.

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

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

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

14 Litigation disputes

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

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

15 Review of contracts by Finance

PRIMARY OBJECTIVE

Contracts and material commitments are reviewed by Finance

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

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

15 Review of contracts by Finance

REQUIREMENTS

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

Link to: Group Delegated Authorities, Finance Policy, Procurement Policy, Lease Directive, Capex Directive, Foreign Exchange (FX) & Interest Rate (IR) Risk Management 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 proper validity, filing and timely renewal of titles, licenses and permits

RISK

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

IMPACT

- Compliance
- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

- 1. Annual approval by the relevant country ExCo member of the list of all relevant permits and licenses for the business to operate, and sign off by the country CEO of exceptions or potential issues. *Annual***
- 2. Annual approval by the country Legal team (or equivalent at your organization), the Quarry (Mine Planner) and Land Management Officer (or equivalent at your organization) of the existing titles of ownership, mining and surface rights, concessions and permits, including upcoming renewals. *Annual***
- 3. Approval, half yearly, by the Land Management Officer (or equivalent at your organization), jointly with quarries management, of the land ownership situation, including proposed or planned land activity (acquisition, disposal), and the effect on the relevant licenses. *Half year***
- 4. Annual approval by the relevant stakeholders of the progress of the mining activities and the compliance with mining regulations and permit requirements. *Annual***

REQUIREMENTS

- For all relevant permits and licenses (e.g. environmental, archeological, operating permits, quarry and mining, production, energy use, vessels and ports, construction, air, water, deforestation, blasting), roles and responsibilities are clearly defined within the organization, adequate processes are put in place in order to ensure their validity, proper filing and archiving, timely renewal, and publication (if required). The list is updated and clear ownership is assigned together with a procedure for management of different types of permit and licenses. (Step 1)
- Local laws and regulations, international standards when required, as well as Holcim Code of Business Conduct (CoBC), are respected in the management of all permits and licenses related activities. (Step 1)
- Third party interfacing with public officials to acquire, renew or review titles, licenses and permits are managed through the Third Party Due Diligence (TPDD) tool (control related to TPDD is covered in MCS 30). (Step 1)
- All existing titles of ownership, mining/surface rights, concessions and permits are reviewed at least annually with the country Legal team (or equivalent at your organization) and in consultation with the Quarry (Mine Planner) and Land Management Officer to ensure they are valid. (Step 2)
- The Land Management Officer leads a review of the land ownership situation twice a year (or according to the local requirements). A review of the foreseen land acquisition/disposals is led by the Land Management Officer with the quarry management and the country's raw material competent person. These reviews cover all requirements to maintain the relevant licenses and permits. (Step 3)
- Renewal of permits, trigger and exercise of mining rights and permits occur before the expiration date. (Step 3)
- Meetings with all stakeholders are conducted to review the progress of the mining activities, monitor compliance with the mining regulations and permitting obligations. These include quarry and plant management, sustainable development, environment, legal and land management. (Step 4)

Link to: Code of Business Conduct, Third Party Due Diligence Directive, Technical Recommendation: Land Management 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, restoration and rehabilitation requirements are implemented for every quarry and properly recorded in financial statements

RISK

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

IMPACT

- Reputational damages
- Operational disruption
- Errors in financials

CONTROL & FREQUENCY

- 1. Annual reconciliation of the resources and reserves with the total of extracted tonnages transmitted to the Accounting department based on the yearly estimates and approval by country CFO. Cases where the remaining useful lives of plants and equipment are greater than the remaining secured reserves must be reported in the Financial Certification package. *Annual***
- 2. Annual verification by Finance and land and quarry management of the validity of the restoration/rehabilitation concept and costs, as well as the assumptions used to calculate the provisions. *Annual***
- 3. Verify if the quarry is classified as high biodiversity importance according to criteria for biodiversity importance category (BIC 1 and 2). If yes, annual review of Biodiversity Management Plan (BMP) by an expert to ensure that actions being implemented properly address the site biodiversity issues. Verify that the Biodiversity Index (BIRS) is established for all quarries. *Annual***
- 4. Review and validation by Legal of contracts relating to the rehabilitation/restoration work prior to signing. *Upon request***

REQUIREMENTS

- Reserves for cement production sites must be classified according to the Raw Material Resources and Reserves Reporting Standard. On a yearly basis, raw material resources and reserves as well as raw mix lifetime figures have to be reviewed and validated by a Holcim competent person and reported according to the business cycle requirements defined by the Plant Development Plan (PDP) as per the Raw Material Resources and Reserves Reporting Standard. Aggregates resources and reserves are classified according to HARP definitions. Each country shall report yearly raw material resources and reserves according to the business cycle requirements defined by Aggregates Reserves Management (ARM). (Step 1)
- The yearly estimate of the reserves are reconciled with the total of extracted tonnages transmitted to the Accounting department. (Step 1)
- All resources and reserves acquired are correctly reflected in the accounts and do not lead to any impairment issues. Cases where the useful lives of the plants and equipment are greater than the remaining secured reserves and resulting production lifetime for cement and aggregates sites, the related action plans must be developed and reported in the Financial Certification package. (Step 1)
- A restoration/rehabilitation plan for each quarry operation must be developed according to the Group requirements and in line with the intended long-term development of the quarry site, specifying the magnitude and schedule of restoration/rehabilitation work. The plan and its supporting documents are available from both land and quarry management and Finance. (Step 2)
- The cost of restoration/rehabilitation work, based on local historical data or estimates given by recognized specialists, is verified and approved by the country plant management and is included as an annex to the plan, allowing the assumptions to be verified. (Step 2)
- At least once a year, Finance and land and quarry management, with Legal if necessary, meets to review the validity of

the restoration/rehabilitation concept as well as the evaluation of related costs and validate assumptions used to calculate site restoration/rehabilitation provisions (discount rate, timing of future cash costs, residual life, etc.). If a revision occurs that impacts a legal guarantee related to rehabilitation, Finance will secure the corresponding revision. (Step 2)

- A Biodiversity Management Plan (BMP) must be in place for quarries categorized as of high biodiversity importance according to the criteria for biodiversity importance category (BIC 1 and 2). (Step 3)
- Biodiversity Index (BIRS) must be established in all quarries (active and non-active, including closed sites). (Step 3)
- Materials used for restoration must be compliant to the Health, Safety and Environment (HSE) Internally Generated Waste Standard. (Step 4)
- Restoration/rehabilitation work contracts must be reviewed on regulatory aspects by Legal experts prior to signing and are copied to Finance for filing. (Step 4)

Link to: Finance Policy, Raw Material Resources and Reserves Reporting Standard, Aggregates Reserves Management (ARM), Criteria for biodiversity importance category (BIC 1 and 2), Quarry Rehabilitation and Biodiversity Directive, Health, Safety & Environment (HSE) Internally Generated Waste standard, Lease Directive, Capex Directive, 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 the proper recognition and classification of fixed assets in the financial statements

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

- Assets are properly classified. Refer to HARP 3.1.1.2.4 Property, Plant and Equipment (PPE), HARP 4.4 Capitalization, Accounting and Valuation of Assets, and HARP 4.2 Accounting for Leases. Lease Directive and CAPEX Directive. (Step 1)
 - Depreciation schedules required for different purposes are maintained. Refer to 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)
 - Capitalization of the expenditure and the timely initiation of depreciation are reviewed and approved by the appropriate Finance person. Journal entries, if needed, have attached the supporting calculation and are signed off by the appropriate Finance person. (Step 1)
 - The person responsible for Construction in Progress (CIP) reviews the status of all Construction in Progress to check whether assets, with a value deemed recoverable, are ready for use. Any change related to the project and the use of the asset should be taken into account in the assessment of the irrecoverability of the asset value. Based on this review, Finance staff responsible for Property, Plant and Equipment (PPE) reclassifies Construction in Progress to fixed assets and initiates depreciation within 30 days of the recorded actual finish date. Any journal entries made are reviewed to ensure proper classification, and approved. HARP 3.1.1.2.4 Property, Plant and Equipment (PPE). (Step 2)
 - Accelerated depreciation of an asset might be required if a tangible asset becomes obsolete, is replaced earlier than expected, or cannot be used anymore as a result of newly introduced stringent environmental measures. (Step 3)
 - Once assets are identified as unused, mothballed or idle, the depreciation and the assumptions should be supported by adequate documentation and properly approved by the CFO (or designee). Unused, mothballed and idle assets that have been written off are supported by adequate documentation and approved by the CFO, as well as change of depreciation method (including reduction of useful life). 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 might trigger additional investment in proven technologies resulting in certain assets being idle or obsolete in a shorter period than the original estimated useful life of the assets. This should be reviewed carefully with the region Head of Finance and accelerated depreciation might have to be accounted for. (Step 3)
- Link to: Finance Policy, Lease Directive, Capex Directive and Annual ARC impairment model and impairment testing guidelines**

19 Physical verification of fixed assets

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

- Regular physical inventories of assets are performed on a rolling basis (at least once every three years) and differences in floor to list and list to floor comparisons are identified. Material differences are analyzed to identify their

root causes and implement corrective actions. Any adjustments need to be documented and approved by the CFO before being recorded. (Step 1)

Link to: Finance Policy

Revenue



20 Management of customer and material master data

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Compliance
- Reputational damages
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

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

21 Price management

PRIMARY OBJECTIVE

Prevent unauthorized changes to prices, discounts or rebates

RISK

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

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

- All price determination processes are defined in a local written and regularly updated (as a minimum every three years) pricing policy and formalized in sales contracts and/or sales orders, compliant with legal requirements as well as fair competition and anti-bribery and corruption laws and regulations. A price list of all products and services is set by Pricing, Sales and Marketing, taking into account different pricing aspects as per the local pricing policy, including other providers (e.g. transporters, applicators). A complete list, including effective dates, is communicated to the responsible team for updating the list in the system. No backdating of effective prices is allowed. (Step 1)
- Standard discount and rebate structures are defined for different categories of customers. Each type of discount or rebate is outlined in the company's policy with defined objectives and clear application rules, all approved by management and backed by local Legal and Compliance. No backdating of discounts and rebates schemes is allowed. (Step 1)
- Exceptions to standard discounts/rebates are specified in accordance with the company's policy and are authorized by the designated approver. (Step 1)
- 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 (SoD) within the Commercial function, properly approved, accurately reflected in the system and exception reports are leveraged and reviewed before the sale. Corrective actions are duly closed within the process of the company's policy and documented. (Step 1, 2)
- Pricing master data change report available at each region/country is reviewed. (Step 3)

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

22 Control of customer credit limits

PRIMARY OBJECTIVE

Grant prior authorization for customers exceeding their credit limit

RISK

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

IMPACT

- Compliance
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

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

23 Matching of sales orders, shipments and invoices

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

23 Matching of sales orders, shipments and invoices

REQUIREMENTS

- All sales orders, shipments and invoices are recorded in the applications. (Step 1)
- Accuracy of amounts invoiced are checked when manually calculated, or are accurately calculated by the application system using standard programed algorithms and established terms of sales (unit price, discount and rebates rate). (Step 1)
- Invoices/billing (e.g. quantities, price, discount, rebates, product, customer data) are matched with sales orders, quantities shipped and customer master file information. An automated match is performed between the invoice and order (including all necessary data). (Step 1)
- Any differences are investigated and related adjustments are approved and documented (e.g. returns, redispach, interco mismatch, cut-off). There is a pre-defined tolerance threshold at the weighbridges for dispatched goods. In addition, any discounts and taxes match the approved parameters in the system from sales order to invoice. (Step 1)
- At least annually, weighbridges and measurement equipment are re-calibrated as per local regulations. (Step 2)
- There is, at least at month end, a follow-up on unbilled items. The report of unbilled items is reviewed weekly (or in line with the locally defined frequency of customers' invoicing) by the billing team, and all the unbilled items are billed within one week from the date they first appear in the unbilled report and within the same reporting month as the delivery. Every month end, the Sales Manager receives the information, documenting any follow-up action. (Step 3)
- SAP: all orders shall be processed via SD module, including any discounts and rebates (i.e. no direct FI bookings). (Step 4)
- Finance verifies and approves the need for a possible adjustment entry (e.g. sales accrual) at the end of the month, based on the unbilled items. (Step 4)
- Rules for closure of open sales orders with delivery date in the past must be defined locally in accordance to the sales terms and conditions, but should be resolved half yearly, at a minimum. (Step 5)

24 Accounts receivable valuation

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

- The bad debt provision must consider the risk of debt recoverability at the end of the reporting period every quarter: (Step 1, 2)
 - quarterly reconciliation of trade balances with the customers must take place, and documentation kept to demonstrate effort to collect the receivables (formal dunning process and exchanges with the trading partner),
 - the assessment of the bad debt provision is estimated using an expected credit loss (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 receivables, prepaid expenses and other current assets (IFRS 9),
 - any change is clearly documented and justifiable by the country,
 - provisions are reviewed and approved by the appropriate country Finance person and recorded by the designated department, and
 - the Credit Committee meetings are held regularly (at least quarterly) to monitor the doubtful accounts receivable balances.
 - Review over specific Accounts Receivables which indicates uncollectibility is considered for write-off. Uncollectibility is evidenced by significant difficulty of debtor, a high probability of bankruptcy or other situations as defined in Holcim Accounting and Reporting Principles (HARP): (Step 3)
 - write-offs are determined by the Credit Committee on the basis of appropriate supporting documents,
 - write-offs for amounts above a locally defined threshold are approved by the country CFO, and
 - if receivables are collected after being written off, the amounts collected should be directly credited on the company bank account and the information provided to the Accounts Receivable department.
- Link to: Group Delegated Authorities, Finance Policy and HARP 3.1.1.1.5 Accounts Receivable Trade**

Human Resources



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

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

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

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.

CONTROL & FREQUENCY

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

REQUIREMENTS

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

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

REQUIREMENTS

Human Resources System Master Data Management:

- after the go-live in SuccessFactors, an Employee Master Data management process that defines roles, responsibilities and rules for employee data management must be in place, and quarterly reviewed to ensure quality, security, and compliance. All existing employees must have complete records in SuccessFactors in accordance with the data governance matrix. The hiring process should be enhanced (modify) and automated as much as possible to fulfill the requirement of this step, (Step 4)
- adding or changing a new employee data requires appropriate approval based on an employee change request with supporting documentation. Each HR entity must identify the mandatory supporting documentation as per local regulations. A check is performed to confirm that all required information is complete and accurate. Changes to Employee Master Data in SuccessFactors must follow the standard Group People Library (Human Resources definitions). These changes should also 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 run of all creations, modifications and deletions to ensure that authorized users duly approved and performed all the changes. If any exceptions are found, they are documented and reported immediately

for investigation by the Group HRIS team. Corrective actions are documented and tracked. All exceptions are closed within the next two weeks, (Step 4)

- at least monthly, the entity's Human Resources team must reconcile the employee data between SuccessFactors and the local payroll system to ensure data consistency (procedure). The employee movements (hire, transfers, promotion and departure) are reviewed to ensure that they are recorded correctly in both systems. Discrepancies are to be corrected within 30 days, and (Step 5)

- only authorized users from the Human Resources department have access to manage employee master data in SuccessFactors and employee data in the local system for employee data management (procedure). (Step 6)

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

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

26 Payroll

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

- Approval prior to processing payroll: (Step 1)
 - balancing routine control: for manual and mass uploading imports, the Payroll Manager should perform data accuracy controls (e.g. verify that the input of total hours worked received from the manager matches with the total hours worked indicated in the payroll system, verify that the total amount of bonus received from Human Resources matches with the total amount in the payroll system). In case of payroll system integration with any other system, the interface should ensure data approval from the source,
 - when bonus or any other payout is processed (with or without payroll), secondary approval should be performed to ensure accuracy of payout, both at individual and total amount to be paid, and
 - analytical review comparing one month to another justifying variance (if any) is performed before bank transfer. The analytical review covers payroll

- exception reports to identify unusual amounts (e.g. negative value check, zero value check, significant increase between two months, etc.).
- Reconciliation after processing payroll: for each payroll, the total payment issued (Treasury account) is reconciled with the payroll journal in order to check that the amount paid to employees matches with the amount calculated by the Payroll department. (Step 2)
- At least every six months (e.g. during salary and bonus review and budget, MTP or forecast cycles), or more frequently if risk is identified as high, the cost center responsible must validate that the own employee cost being charged to their department is correct (total employee cost). High risk countries are identified by the region Human Resources Director in coordination with the region Internal Control responsible. Any discrepancies found should be resolved within 30 days. (Step 3)

Link to: Human Resources Policy

27 Compliance with payroll and local labor laws

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Reputational damages
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

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

28 Employee pension and benefit plans

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

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

28 Employee pension and benefit plans

REQUIREMENTS

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

- Section 4.1 of the Directive sets the rules for design of pension plans and other post-employment benefits which should be in accordance with the local regulations and market practices.
- Approval rules to be followed are defined in section 4 for each activity (e.g. closing and freezing pension plans, de-risking liability management, de-risking investment strategy, employer funding contribution, etc.).
- Reporting for post-employment defined benefit plans should follow the process as per instructions from Group Accounting, Reporting and Consolidation (ARC). Actuarial methods and assumptions to be used should be aligned with the instructions.
- Reporting should be updated in AON tool, Risk Analyzer (RA) as per the instructions for the relevant plans. The local actuary should upload the information related to benefit plans

together with actuarial report. The CFO (or designee) should review and sign off the results and accounting entries. The CFO (or designee) should have control over inputs (mainly employee data), and the outputs (analytic review of the main parameter and final results), in addition to the control performed over the assets valuation.

- The Group oversees the management of its pension plans through the Pension and Benefits Governance team (PBGT). This interdisciplinary team including Finance, Human Resources and Legal specialists acts as a center of expertise in all issues relating to pension and other post employment benefits and makes recommendations to Group management. The sponsor (local company) has to inform to the Pension and Benefits Governance team of any project of new plans or amendment of current plans, and request approval as per the Group Delegated Authorities (GDA).

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

Expenditure



29 Management of supplier master data

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Compliance
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

- A supplier master data management process that defines roles, responsibilities and rules is in place and reviewed when required. (Step 1, 3)
 - Duplicate check is performed before a new record is created. Duplicate records are not permitted. Each entity should formally define its mandatory and critical fields in SAP or local ERP, in line with the legal and business requirements. The list should include, as a minimum, legal name, bank details, incoterms, reconciliation account (General Ledger), and control data (Goods Receipt-based invoice verification). Other fields can be locally added above the minimum. (Step 1)
 - The onboarding of new suppliers needs the submission of a supplier registration form and appropriate supporting documentation. Specifically, the incorporation of bank account details relies on the provision of these documents. Acceptable forms of supporting documentation include: RIB, IBAN, a bank letter of confirmation, a canceled cheque displaying the vendor's name, or a bank statement. A verification process must be conducted to ensure that all required information and documentation is complete and accurate. (Step 1)
 - For existing vendors, any changes to bank account details must be supported by appropriate approvals and relevant supporting documentation, in addition to the supplier's request for change. Acceptable forms of supporting documentation include: RIB, IBAN, a bank letter of confirmation, a cancelled cheque displaying the vendor's name, or bank statement. The new bank details can only be updated after completing a callback process using the registered contact information in the master data. The master data management team must document the call through either a follow-up confirmation via email or a recorded call. Alternatively, the callback process may be replaced with direct verification of bank account ownership through bank portals, when this option is available. A verification process must be conducted to ensure that all required information and documentation is complete and accurate. (Step 1)
 - Quarterly, a master data change report is run of all creations and modifications to ensure that all the transactions were performed by authorized users based on approved requests and documents. (Step 1)
 - If any exceptions are found, they are documented and reported immediately for investigation. Corrective action is documented and tracked. All exceptions are closed in a timely manner (locally defined). (Step 1)
 - Supplier records are to be reviewed on an annual basis for data quality (duplicate check, tax code check, bank account check, mismatch in the supplier and bank account country, and inactive suppliers for more than 18 months), and are deactivated or blocked for payment and purchase, with the exception of Solutions & Products' suppliers (warranty program). Suppliers identified as part of the procurement supplier reduction strategies are to be deactivated and flagged for deletion. (Step 2)
- Link to: Procurement Policy**

30 Supplier qualification and claim management

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Compliance
- Reputational damages
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. Screening of potential suppliers by Procurement (or designee) based on the criteria required by Procurement, Sustainability, and Compliance including sanctions and Third Party Due Diligence, must occur prior to entering into a transaction or adding a supplier in the supplier master data or approved supplier list.

Upon request

2. Review of supplier performance by Procurement must occur for critical and strategic criteria (including suppliers with high ESG impact). Suppliers not meeting the requirements are flagged as 'disqualified' or 'conditionally approved' until action plans are completed, or the supplier is blacklisted if there are ongoing issues. Annual

3. Supplier qualification must be updated at least on an annual basis for critical and strategic suppliers (including suppliers with high ESG impact). Annual

REQUIREMENTS

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

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

PRIMARY OBJECTIVE

Reconcile purchase orders, receipts and invoices (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 & FREQUENCY

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

REQUIREMENTS

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

- purchasing instruments (purchase request, purchase orders, framework orders or contracts) are approved according to country, regional and Group delegations of authority (involving Legal and Finance departments when required) prior to entering into a commitment with the supplier, (Step 1)
- supplier invoices are only cleared for payment after the system automatically matches the purchase order, receipts and the supplier invoice (three-way match), or the purchase order and an approved invoice (two-way match), (Step 1, 2, 3)
- discrepancies between the invoice, purchase order (PO) and receipt, are formally identified and the system blocks the payment process if the discrepancy exceeds the locally defined threshold. Defined thresholds must be documented and approved by local delegation of authority (DoA), and (Step 2)

- an exception report (exception to three-way and two-way match) is distributed regularly for verification and resolution. Only when the exceptions are cleared and properly explained, the payment can be made. If discrepancies exceed a defined threshold, payment requires approval as per the delegation of authority. (Step 2, 3)

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

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

Link to: Procurement Policy

32 Payment processing

PRIMARY OBJECTIVE

Approve payments and cash disbursements 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 & FREQUENCY

- 1. Approval according to the Group Delegated Authorities, the local delegation of authority and related directives, of all payments and cash disbursements, prior to payment. *Upon request***
- 2. Expenditures falling in the gift, hospitalities, strategic social investments, sponsorship and donations, entertainment and travel, and expense categories, are identified through the accounting system. Payments carried out in contradiction to the Gifts, Hospitality, Entertainment and Travel, or Strategic Social Investment, Charitable Sponsorships and Donations Directives, are rejected. *Upon request***
- 3. Monthly review and approval by the designated Finance person of the accounts payable subledger accounts and the aging report to examine unusual balances and take corrective actions. *Monthly***

REQUIREMENTS

- Payments and cash disbursements are approved according to the local and Group Treasury Directive, Group Delegated Authorities (GDA) and the local delegation of authority, prior to actual payment. (Step 1)
 - Payments related to transactions that did not go through the purchase order (PO) or direct invoice (FI) process, are authorized on the basis of appropriate supporting documents and according to the local delegation of authority (DoA) prior to actual payment. Acceptable supporting documents for manual payment requests are: invoice including IBAN or bank details, agreement/contract including IBAN or bank details, official document of the local authorities including IBAN or bank details, official online registry of bank detail or IBAN verifiers (e.g. tax office, or companies registry). Where they exist, countries will comply with local regulations. Bank details must be authenticated based on a trustworthy and independent (other than the one provided by the requestor) source of information (two-factor authentication). (Step 1)
 - The payment process ensures that distinct persons are in charge of the following tasks: 1) approval for payment (persons signing the cheque or issuing the payment by bank transfer), and 2) accounting (preparation of bank journal entries). Disbursements should be processed by a staff member independent from the receipt or invoice matching process. (Step 1)
 - Payments to suppliers that represent the company to government agencies, officials or owned-enterprises have been approved under the Third Party Due Diligence Directive (TPDD) before the payment can be made. (Step 1)
 - Sponsorship and donation payments or any payment made directly or indirectly to public officials without expecting any consideration in return must be reviewed by Compliance, and authorized according to the local delegation of authority (DoA), the Group Delegated Authorities (GDA) and the Strategic Social Investment, Charitable Sponsorships and Donations Directive. (Step 1)
 - All business trips require appropriate authorization and controls, to be adhered by both the line managers and employees. The local travel policies shall include an approval system and process in accordance with the Travel and Events Policy. (Step 1)
 - Incorrect payments: a process must be in place to prevent incorrect payments (e.g. use of a report to check for duplicate payments, stamping invoices as paid when the payment is issued, or other automatic system control). (Step 1)
 - Payments made to third parties as marketing gifts, hospitalities, entertainment and travel, above the threshold defined by countries, and to public officials, have been approved according to the rules defined in the Gifts, Hospitality, Entertainment and Travel (GHET) Directive. Reimbursement of GHET payments made in cash are not allowed. (Step 1, 2)
 - Country CEOs' expenses are to be controlled and approved by the area Manager or region Head (could be delegated to the region Head of Finance). If not approved directly in the ERP system, the offline (email) approval has to be attached in the local approval system. (Step 2)
 - In connection with the month-end closing, the accounts payable subledger is reviewed to examine unusual balances (e.g. old balance, debit amount, incorrect currency rate, etc.). Debit balances within the Accounts Payable subledger are reviewed and justification is checked for (e.g. credit notes, advance payments). The follow-up actions are described and monitored in the following month. (Step 3)
- Link to: Group Delegated Authorities, Travel and Events Policy, Third Party Due Diligence Directive, Treasury Directive, Strategic Social Investment, Charitable Sponsorships and Donations Directive, Gifts, Hospitality, Entertainment and Travel (GHET) 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 accruals for expenditures are properly recorded in the financial statements in the correct period

RISK

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

IMPACT

- Errors in financials

CONTROL & FREQUENCY

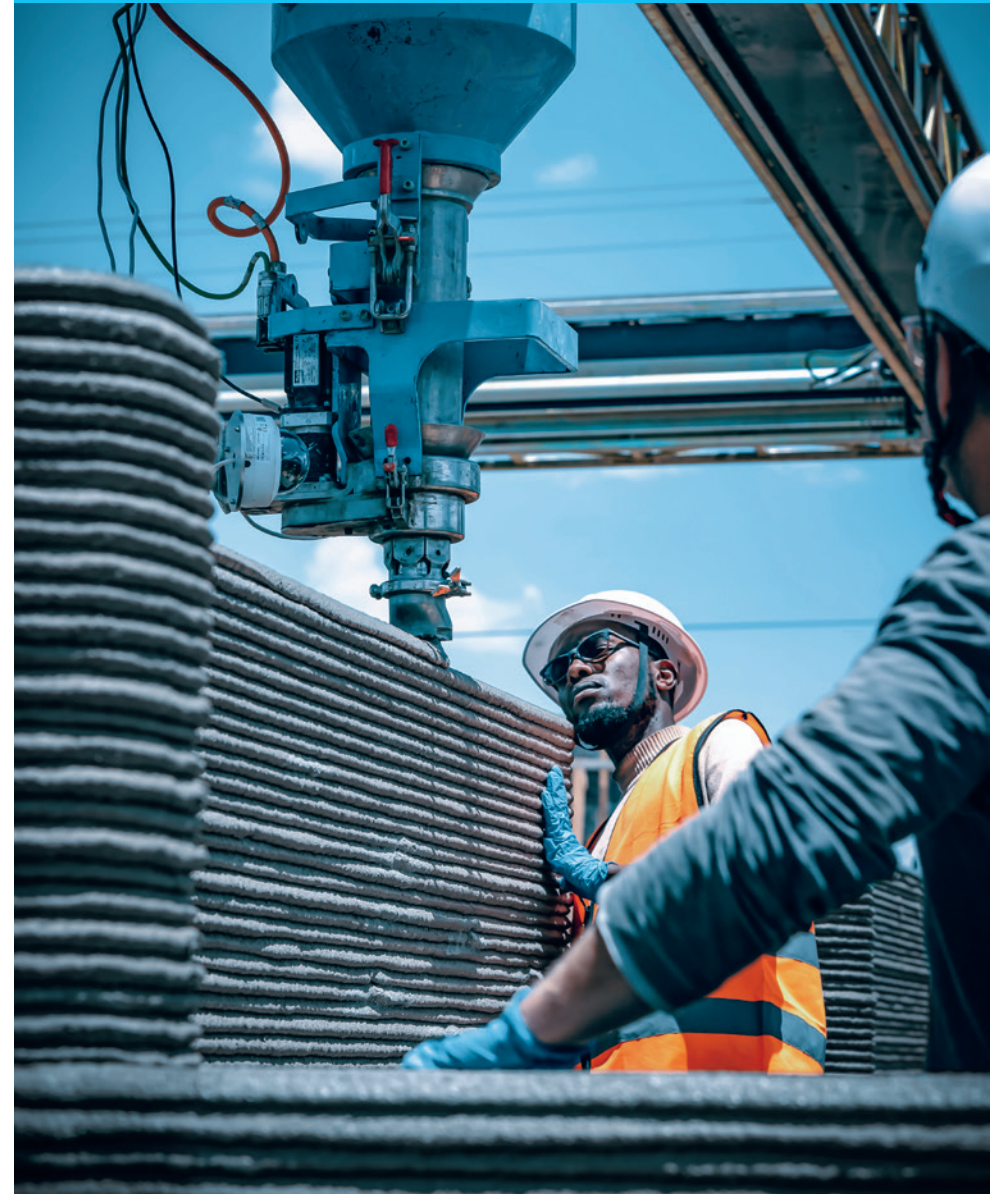
1. **All goods receipt (GR) and services receipt (SR) should be recorded before the month end by the responsible locations. Purchasing manager (or designated) should verify that there are no unrecorded goods receipt or services receipt at the month end for the goods and services received as per the purchase orders. *Monthly***
2. **Goods receipt and invoice receipt (GR/IR) account (or equivalent system account) should be cleared monthly (ongoing), before month end closing by the designated person (business or Procurement). *Monthly***
3. **Accruals are booked monthly by the Accounting function for all purchases and expenses with pending invoices. Any adjustment to the accruals needs to be approved by the appropriate Finance responsible. *Monthly***

REQUIREMENTS

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

Link to: Finance Policy

Inventory



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

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

Regular physical stock takes of parts and supplies and materials are organized by the Operations team, with participation of the Finance team, and performed according to defined procedures. Any other approach due to business restrictions or particularities must be agreed in advance and approved by Group Internal Control.

PARTS AND SUPPLIES (Step 1)

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

• Preparation of physical inventory

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

• Stocktake

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

• Frequency

The stock take of parts and supplies is to be performed at least yearly. In case that full scope stocktake of parts and supplies is not performed at the year end, monthly

or quarterly cycle counts are organized, and ensure that all parts and supplies were included in the yearly stocktake process.

• Roles and responsibilities

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

• Follow-up on stocktaking results

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

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

REQUIREMENTS

MATERIALS (Step 2, 4)

Materials include raw material, fuel, semi-finished, and finished goods

• Preparation of physical inventory

- The plant procedure for stocktaking which describes scope, objective, resources and timeline, is available and applied.
- There is a layout map to show the scope of the stock take. Off-site stocks are included.
- The stock take planning is validated by the Plant Manager and communicated to all stakeholders.
- Movement of goods is stopped or controlled during the stocktaking (reception, issue, return, etc).
- Date and time of measurements have to be recorded.
- Calculating formulas should be established and declared.
- All the measured figures must be reconciled from the time and date of the measurements to the end of the month at 24 hrs.

• Stock take

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

• Specific matters

- **Measurement methods and instruments:** measuring methods and instruments must be optimized at the maximum to ensure the reliability of the measures.

- **Equipment calibration:** dosing equipment and weighing devices should be calibrated regularly following a defined schedule. Perform at least four calibrations annually for weight feeders in raw and cement mills, as well as for fuel and kiln feed dosing devices. All calibration measurements must be accurately documented, with records maintained for at least one calibration per device following its annual overhaul.

- **Heaps geometry:** whenever possible, shape all bulk material heaps into regular geometric forms. Before stock counts, the Production Manager and Mining Engineer must confirm the geometric shape and zero levels of all major heaps.

- **Densities:** the bulk density of all materials, in both loose and compacted forms, should be measured and mutually agreed upon. Each stockpile, whether loose or compacted, must use the corresponding density. Bulk densities should be verified annually or confirmed to remain unchanged (i.e. no alterations in material source or quality).

- **Moisture:** each site should have a clear procedure outlining the steps for conducting moisture analysis. Moisture analysis must be performed regularly on all raw material and solid fuel deliveries, with results properly documented and stored.

- **Solution & Products:** for business and sites within the Solutions & Products segment (i.e. concrete products, mortar solutions, asphalt, construction and paving, roofing, retail, etc.), where the number of inventory materials codes (SKUs) is exceptionally high, materials might be counted through monthly cycle counts. The material codes included in each cycle count will rotate based on a predefined inventory classification methodology formalized in the local procedure. This methodology prioritizes inventory management and control

REQUIREMENTS

using criteria such as value, demand, and usage. The chosen methodology must be justified by the business's characteristics, inventory size, and objectives, and be reviewed and updated on a yearly basis. Cycle counts will ensure that all material codes in inventory are covered at least once within a one-year cycle. Where the business context permits closer monitoring and tighter control, a stricter and more frequent counting approach should be adopted.

• Frequency

- The raw materials, fuels, semi-finished and finished goods stock take is performed by Operations on a monthly basis. At least once per year, the stock take should be performed by an independent expert (e.g. third party surveyor or other functions when necessary). Third party survey is mandatory if: i) there is local legal requirement, or ii) business has a challenge to ensure adequate physical inventory due to lack of skills, tools or internal resources.

• Roles and responsibilities

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

- Plant Managers and Manufacturing Directors or Business Line Managers, as per the local DoA, are responsible to review and approve production and stock adjustment proposals.

- Finance Controller (or independent designee when necessary) ensures reliability of the work done. Finance/Controlling participates on the stock measurement monthly. Finance (or independent designee when necessary) must participate on the field as part of the count team at least half yearly. The Finance controller is overall responsible for the compliance and reliability of the stock reconciliation process locally performed in the plant and, when necessary, records adjustments to the financial statements according to the defined DoA.

• Monthly stock reconciliation (Step 3)

- An end-of-month production data reconciliation is performed by the Production Manager (or delegated person).
- Stock reconciliation is done between all materials stock measured values, products delivered, materials received, and production/consumption figures for the current month. Reconciliations should be performed on a dry basis for semi-finished and finished goods, on a wet basis for the other materials (raw materials and fuels).
- The following parameters cannot be adjusted and must be considered as fixed: semi-finished and finished goods tonnages (shipments, deliveries and physical measures of stocks), total operating hours for the month for each semi-finished and finished goods manufacturing equipment.
- All material physical quantities from stock take inventory are cross-checked with stock information in the data system (TIS and other systems) by independent people (not those in charge of material stock take).

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

REQUIREMENTS

- Discrepancies between the measured physical stock and stock information in the ERP system for all physical stocks must be analyzed first and before proceeding with adjustment of production inputs, reliability of the information system, accuracy of stock take and output of the manufacturing lines for the month. A double count is performed in case of quantity discrepancies above 5%.
 - Discrepancies are analyzed to identify their sources and implement corrective and preventive actions. Any discrepancy above 5% for semi-finished and finished goods need to be investigated and documented with justifications.
 - No adjustments to be made in the data system (TIS, SAP or JDE) without the approvals as per the local DoA. The same users should not be allowed to make adjustments in the production tools (e.g. TIS for cement sites) and ERP (e.g. SAP, JDE) inventory modules.
 - **Changes in TIS over critical fields:** a TIS data change report (i.e. DataCorrLog) is generated quarterly to capture and review all modifications. The Finance Controller evaluates the report to verify that all changes were made by authorized users in accordance with the local DoA and based on approved and documented requests. Any exceptions identified are immediately documented, 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: i) raw meal to clinker factor or kiln feed to clinker factor (depending on the cement plant's methodology), and ii) moisture content for all inbound materials (e.g. solid fuels and raw materials). Additional fields may be included locally, beyond these minimum requirements.
 - **Raw meal to clinker factor / kiln feed to clinker factor determination:** the Finance Controller performs a quarterly review to ensure formal evidence is available 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 always be properly justified. All new factor value determinations must be formally documented and jointly approved by the Process Engineer, Production Manager, and Plant Manager.
 - **Dead stock:** for all bulk materials, the total stock taken into account in the production data report includes the 'live stock' (movable automatically with permanent equipment) and the 'dead stock' (non movable automatically). The value of the dead stock is agreed upon between the Production Manager and the Finance Controller.
 - **Zero and full stock:** for bulk materials, it is recommended to reach at least once a year a physical zero stock level in order to perform a consistency check between theoretical stock and physical stock. When a full-stock or zero-stock level is reached, discrepancy between book and physical stock must be adjusted.
- Link to: Finance Policy, HARP 3.1.1.1.6 Inventories and HARP 3.2.1.2.30 Inventory Movements Finished Products**

35 Inventory valuation

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

- The valuation of each type of inventory is reviewed for consistency with HARP. Inventory costs include purchasing costs, conversion costs and other costs incurred in bringing the inventories to their present location and condition (excluding storage costs). (Step 1)
 - Purchased products are valued at the purchase price less any price deductions, such as trade discounts and rebates. Expenses directly related to the acquisition (insurance, import duties, transport and handling costs, etc.) are included in the value of the inventory. (Step 1)
 - Inventory of own produced finished and intermediate products are valued based on actual cost of goods produced including depreciation and certain distribution costs (transport to terminals, warehousing, bagging, etc.). Standard costing can be used during the year. At year-end, inventories must be restated to the actual cost. Standard cost should be updated, at a minimum, once per year at year end (or for November hard close). (Step 1)
 - Inventory provisions (obsolescence and slow moving of spare parts) and write-offs, are estimated according to Holcim Accounting and Reporting Principles (HARP), based on appropriate supporting documents and applied consistently from one year to another. They are approved according to the local delegation of authority. (Step 2)
 - The review for obsolescence for slow moving parts, and related provisions and write-offs, is performed half yearly during hard close events. (Step 2)
 - The inventories of raw materials and kiln fuels (coal, petcoke, oil, etc.) with no movements for more than three months must be valued at the lower of costs and net realizable value per location 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**

IT



36 Management of access to IT systems

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Operational disruption
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

Note: Information Technology (IT) systems refers collectively to business applications and IT infrastructure (operating system, database, network, interfaces).

Granting/Changing Access: (Step 1)

- a formal user access request form should be filled out for every new or change request to Holcim information systems, and the corresponding approver has to approve it ensuring compliance with segregation of duties (SoD) rules,
- Human Resources should confirm the identity of all internal users, and the Holcim sponsor for external users, and
- external user IDs and temporary Holcim employees must have a defined expiration date up to twelve months

(renewable). Based on the type of ID and associated risks, the sponsor may choose to further limit this expiry to a shorter period (e.g. three months). Expiration may be set up at Google or active directory level where not supported by the application.

Termination: (Step 2)

- the scope of this control starts from the time Human Resources or business notifies IT a request for termination of the user. The control for business notification to IT is under MCS 25. IT has to revoke access within defined timeline upon Human Resources or business notification.

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

37 Review of IT user access rights to production IT systems

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Operational disruption
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

Note: Information Technology (IT) systems refers collectively to business applications and IT infrastructure (operating system, database, network, interfaces).

- This control must cover the review of all Information Technology (IT) function users (e.g. OS, DB and Network administrators, AD administrators, application support team from IT, and all other IT users who have access to production IT systems). Access review of

business users to IT systems is covered under MCS 12 and, therefore, not in the scope of this control. (Step 1, 2, 3)

- An IT user cannot review their own access. The review confirms that access is in line with the IT users role and responsibilities. (Step 1)

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

38 Security configuration settings and batch job management

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Operational disruption
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

Note: Information Technology (IT) systems refers collectively to business applications and IT infrastructure (operating system, database, network, interfaces).

- Minimum Security Baseline requirements are defined in Annex 09.01: Holcim Minimum Baseline Security Standard, and approved by the Group IT Security responsible. (Step 1)
- ITSC Security Officer is responsible to obtain the IT system configuration settings and review them to ensure they are as defined (or stricter) in the security configuration baseline. (Step 1)
- For IT systems not managed by Holcim (e.g. cloud hosted and managed by third parties), business or IT should obtain

an independent audit report (e.g. ISAE 3402) from the service provider at least annually to verify and follow up on any IT internal control deficiency reported. (Step 1)

- Critical batch jobs (different from end user scheduled background jobs) are identified (e.g. interfaces between Enterprise Resource Planning and other critical systems) to ensure if failures exist; if any, they are timely corrected to ensure data integrity. Access to such scheduled jobs is restricted. (Step 2, 3)

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

39 Data backup, storage and restoration process

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Operational disruption
- Financial loss

CONTROL & FREQUENCY

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

REQUIREMENTS

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

- scheduling,
- backup rotation,
- retention times,
- testing of restoration process,
- evidence that backups are performed, and
- evidence of tests performed regarding the restoration procedure.

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

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

40 Managing changes to IT systems

PRIMARY OBJECTIVE

Prevent unauthorized changes in IT systems

RISK

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

IMPACT

- Operational disruption
- Financial loss

CONTROL & FREQUENCY

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

REQUIREMENTS

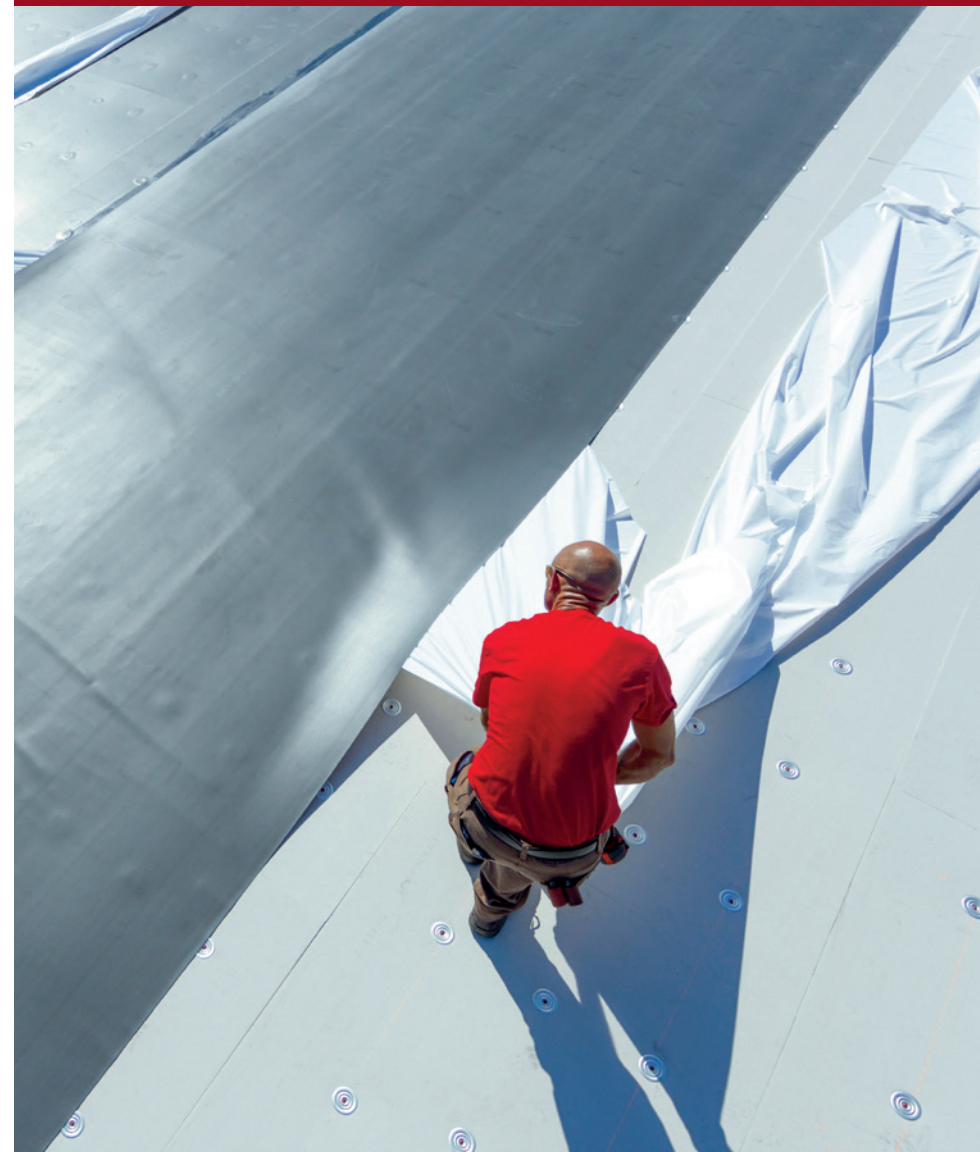
Note: Information Technology (IT) systems refers collectively to business applications and IT infrastructure (operating system, database, network, interfaces).

- Changes to IT systems should be requested only by authorized approvers (application super users, business process owners) to ensure that only valid changes for business needs are requested. (Step 1)
- To request changes, a defined procedure is followed where the approvals are captured and recorded. (Step 2)
- User Acceptance Test (UAT) should not be performed by the developer or change responsible, to ensure a proper task segregation. User Acceptance Test is generally performed by the application super users or business/function approved testers. (Step 3)

- The Change Approval Board (CAB) verifies all changes before providing release approval. Changes should not be moved to production without approval. (Step 4)
- Developers should not have 'change access' to the production system. The changes in the production environment should be moved by administrators (BASIS for SAP ERP). (Step 5)
- Post change monitoring is performed to ensure the changes were correctly implemented. (Step 6)

Link to: Information Technology Policy, Information Systems User 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 all Holcim Accounting and Reporting Principles (HARP) and with regulatory requirements on extra-financial disclosure

RISK

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

IMPACT

- Errors in financials
- Reputational damages

CONTROL & FREQUENCY

- 1. Confirmation by the CFO of compliance to Holcim Accounting and Reporting Principles (HARP) and International Financial Reporting Standards (IFRS) through the financial certification. Any deficiencies identified in a sustainability review conducted by the Group Standards and Accounting Principles (STAP) team are remediated as per the agreed timeline. *Annual***
- 2. EU Taxonomy-aligned activities and related CapEx projects are assessed and documented in Group EUTA tool and signed off by the CFO (or designee). EU Taxonomy-related financial reportings are performed according to Group ARC instructions under the supervision of the Country EU Taxonomy Finance Coordinator. *Annual***

REQUIREMENTS

- The country CFO is responsible for ensuring that HARP are sustained in the company, including updating the internal policies for the HARP change releases. Adherence to Group standards is included in the annual certification letter. (Step 1)
- The Holcim accounting and reporting principles and rules must be implemented in the Enterprise Resource Planning (ERP) systems (SAP, JDE, etc.) of all Holcim Group companies. This implementation is certified by the STAP team, who conducts a detailed review. (Step 1)
- Each Holcim Group company must have an appointed responsible for HARP (HARPist). The CFO is responsible to appoint the HARPist, who is an integrated member of the HARPist Virtual Organization, an extension of the STAP team. The HARPist must be recorded in the company list. (Step 1)
- Regular HARP compliance reviews (7.4.4 HARP Sustainability Review) 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 that are relevant for Group reporting purposes. In the case where local circumstances dictate that a specific IFRS, which is not documented in the HARP manual, is applied, it is the responsibility of the country CFO to ensure that the IFRS is followed (in addition to HARP). (Step 1)
- When the country has a plan to align with the EU Taxonomy, it tracks in its PDPs and MTP the forecasts for aligned sales, as well as action plans to align with or maintain alignment with the 'Do No Significant Harm' criteria. The country's EU Taxonomy Finance Coordinator is appointed and responsible for organizing the assessment of EU Taxonomy-eligible activities in the Group EUTA tool, as well as ensuring the quality of extra-financial and financial data for EU Taxonomy reporting through CapEx (One PPM, where applicable) and financial reporting (in SAP Financial Consolidation, SAP-FC). Any inaccuracy or incompleteness must be disclosed to the 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

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

.....

RISK

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

IMPACT

- Errors in financials

CONTROL & FREQUENCY

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

REQUIREMENTS

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

Link to: Finance Policy and Lease Directive

43 Reconciliation of bank accounts

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

- A proper segregation of duties (SoD) is in place between reconciliation, booking and approval activity. The person who performs the bank reconciliations must not have access to recording of transactions in the accounting system or to process cash disbursements or receipts. (Step 1)
 - At least monthly, all bank statements are reconciled to the general ledger account timely. The accounts denominated in foreign exchange rates (FOREX) are recalculated according to the month-end rate and the impact is recorded in the general ledger. The bank statement, the general ledger (GL) balance and the related journal entries are attached in the bank reconciliation. Reconciling items (identified differences between the book and bank balances) are followed up timely and aged. Any adjustments required to the general ledger are recorded before closing. All bank reconciliations (even for inactive or dormant accounts) at each month-end closing are reviewed and approved by the CFO (or designee). (Step 1)
 - Local banking regulation over clearance of bank transactions has to be taken into consideration for quick identification of unreconciled items. (Step 1)
 - All reconciling differences should be identified, explained and, when applicable, appropriate action for resolution formalized. Any necessary journal entries to resolve the differences should be posted no later than ninety days after the reconciliation is performed. The bank should be contacted concerning any bank errors which should also be resolved within ninety days. The usage of suspense accounts is not allowed. (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 partner to ensure accuracy of the general ledger and proper elimination upon consolidation

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

1. **Signed contract documented and filed for all intercompany transactions. *Upon request***
2. **Monthly review and approval by the designated Finance person of the intercompany and intracompany accounts, including a confirmation with each partner (or documentation that balances agree in Reco-Live). *Monthly***
3. **All applicable intercompany invoices are set to be settled through the netting tool within the defined agreed timing (for Group Reporting Units in scope). *Upon change***

44 Reconciliation of intercompany balances

REQUIREMENTS

- Each intercompany transaction between different legal entities must have a signed contract. Each intercompany invoice must include relevant details for the goods or services provided based on a signed contract. (Step 1)
- All balance sheet and income statement intracompany and intercompany accounts are formally reconciled with each partner unit considering the criterias defined in HARP 7.3.3, including other Group companies. Reconciling items must be identified and corrected before the end of the close. Any Foreign Exchange (FX) difference (between the spot rate and the AV rate) on the cash flow with a Group partner needs to be communicated and documented to Group Corporate Reporting before the publication of the consolidated package. The reconciliations should be reviewed and approved by the designated Finance person. This ensures that intercompany balances are fully eliminated in consolidation. (Step 2)
- Implementation of standardized intercompany settlement process (netting):
 - the netting process and tool (Coproces) covers standardized settlement processes comprising intercompany invoices. There are exceptions clearly defined in the Netting Scope and Principles which reflect limitations of the process and accounting specificities for certain Group Reporting Units (GRU), and (Step 3)
 - every GRU must assess readiness (systems, effort and efficiency) to integrate within a standardized netting process and update their assessment once per three years. The subsequent decision to integrate the new GRU must be approved by the Group Head of Treasury and the netting process owner. (Step 3)

Link to: Finance Policy, Recharges to Corporate Directive, 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 (MJE) are properly supported, reviewed and approved by appropriate personnel

RISK

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

IMPACT

- Errors in financials
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. **Ensure that all manual journal entries (MJE) are approved as per local delegation of authority by the designated Finance person, together with supporting documentation prior to posting. Upon change**
2. **Quarterly verification and sign off by the responsible manager to ensure only approved users from the Accounting function have access to post MJE. Quarterly approval by the countries of a list of approved persons who can request MJE to the Business Service Centers. Quarterly**
3. **Monthly verification and sign off by the CFO (or designee) of the analytical review report of MJE posted. 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/person and are not system triggered/automatic entries in the Enterprise Resource Planning (ERP) application (e.g. accounts payable or accounts receivable ledger posting). MJE are prepared by individuals to capture economic activities outside of subledgers (i.e. directly in the general ledger). When MJE are used, proper process review and approval is in place as detailed below.

- Proper segregation of duties (SoD) lies between MJE requester, approver, and those posting the entries. (Step 1)
- MJE should be posted in the system after they are reviewed and approved. All MJE require approval before posting. Additionally, entries relating to valuation adjustments should be approved by the CFO. (Step 1)

- All MJE are required to have adequate supporting information/documentation, appropriate business rationale, recorded within the right period, and with the right amount. If the entry is performed at a Service Center, this information/documentation has to be provided to them in order for the posting to take place. (Step 1)
- Only users in the Accounting function are allowed to have access to post MJE. (Step 2)
- The CFO (or designee) performs a monthly analytical review of MJE posted (including all required reversals). This includes statistics on the number of entries, nature/type, and amount of MJE to detect any unusual activity as part of the review. Countries define locally the thresholds and unusual items for the review. The reviewer is a person other than someone who is posting the entries. (Step 3)

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

46 Impairment of goodwill, intangible assets and tangible assets

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials

CONTROL & FREQUENCY

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

REQUIREMENTS

Cash Generating Unit (CGU): (Step 1)

- the Group's CGU are defined on the basis of the relevant market normally country or product-related. For the purpose of impairment testing, the Group's CGU are aggregated into an operating segment, which is the level reviewed by the Group CEO (i.e. chief operating decision maker). The operating segments on which goodwill will be tested for impairment would be as follows: North America, Europe, Middle East and Africa, Latin America, Asia Pacific, and Solutions and Products.

Goodwill guidance: (Step 1)

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

Other intangibles with indefinite lives: (Step 2)

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

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

- Group companies shall use the goodwill impairment template at all times when assessing PPE for impairment,

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

Sustainability: (Step 3)

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

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

47 Transactions in a foreign currency

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials

CONTROL & FREQUENCY

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

REQUIREMENTS

- Daily exchange rates published by central banks are usually used to record receivables and liabilities relating to the foreign currency transactions (settlements, recognized gains/losses). The exchange rates 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. utilization of daily rates from the central bank for the last day of the month, instead of the rates communicated by the Group) must be approved by Group Corporate Reporting (ARC) based on 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 a foreign currency transaction (denominated in the currency of the transaction so that the ERP system can automatically revalue the transaction until settlement). (Step 2)
 - Where a transaction is not settled in the same reporting period as that in which it occurred, it must be revalued using the closing rate of the reporting currency. Any resulting gain or loss must be recognized in the income statement as a foreign currency gain or loss. If recorded in the system in the currency of the transaction (foreign currency), this will be done automatically by the ERP system. If not, this must be done manually. (Step 2)
- Link to: Finance Policy, Treasury Directive, Foreign Exchange (FX) & Interest Rate (IR) Risk Management 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 correct scope of consolidation by proper reporting and disclosure of the legal ownership rights

RISK

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

IMPACT

- Errors in financials

CONTROL & FREQUENCY

1. **A new legal entity and/or any changes in the structure of a legal entity must be updated in the Umbrella tool within 3 days of incorporation or change. The Group Reporting Unit CEO and CFO verify the legal entity structure and signs off the Legal Entity Management tool (Umbrella) information half yearly according to Group Accounting, Reporting and Consolidation (ARC) / Group Legal instructions (hard close May and November). *Half year***
2. **Approval by the designated Finance person of the consolidation hierarchy, percentage of ownership and method of consolidation to ensure correct accounting and reporting treatment and reconciliation with 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 (GRU) CEO is responsible to ensure that all legal entities without any limitation of scope, materiality or percentage of participation with direct or indirect control are documented in the Legal Entity Management tool (Umbrella). Sign off by the CEO and CFO confirming completeness and accuracy of reported information performed during the May and November hard close events. (Step 1)
 - All information in the Legal Entity Management tool (Umbrella) is updated within three days after any change occurs. (Step 1)
 - All information in the Legal Entity Management tool (Umbrella) is mandatory and must be uploaded as defined by the Umbrella rules (user guide section 11). (Step 1)
 - Reconciliation over the agreed consolidation hierarchy, with SAP Financial Consolidation (SAP-FC) system and Legal Entity Management tool (Umbrella) to take place whenever a change occurs, or at least half-yearly. (Step 1, 2)
 - On a monthly basis, before the start of the country consolidation, the consolidation hierarchy is reviewed by the local Reporting team to verify the completeness and correctness of the SAP Financial Consolidation (SAP-FC) set-up of the legal entities, the consolidation methods and the legal ownership percentages. In case of changes and/or doubts, alignment with Legal is required and the Group Consolidation (ARC) team needs to be informed accordingly. If the transaction meets the threshold for a change in structure (CIS), it should be reflected in the SAP Financial Consolidation (SAP-FC) package. (Step 2)
- Link to: Group Delegated Authorities, Finance Policy, Treasury Directive, Legal Entity Management Tool (Umbrella) User Guide and Minimum Substance Requirements Directive**

49 Consolidation of financial statements

PRIMARY OBJECTIVE

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

.....

RISK

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

IMPACT

- Errors in financials

CONTROL & FREQUENCY

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

REQUIREMENTS

- A review is performed to ensure the amounts reported in the group reporting package in SAP Financial Consolidation (SAP-FC) are correct and complete. The mapping between the local chart of accounts and the consolidation package, if applicable, is formalized and any change is authorized by the designated Finance person. (Step 1)
 - When a country performs a sub-consolidation, the consolidated reporting package is reviewed for the completeness and correctness of the consolidation, where applicable, including: (Step 1)
 - eliminations, taking into consideration any non-controlling interest calculation,
 - accounting for any deconsolidation, acquisition, merger or transfer, and
 - conversion to the reporting currency and related currency translation adjustment are reviewed for reasonableness using the rates published by the Group (and used in SAP Financial Consolidation).
 - A reconciliation of local equity (general ledger) to the Group consolidation accounts (SAP Financial Consolidation) is performed twice a year (mid year and year end), approved by the CFO (or designee) and uploaded in Umbrella. Differences are explained, documented and recorded. (Step 1)
 - The country reporting package is reviewed and approved by the appropriate Finance person, country CFO, or designee, before being submitted to the Group. The CFO (or designee) formally signs off on the financial statements to confirm that they have been reviewed, that the amounts reported are correct, and that all relevant information for disclosure purposes has been included in the appendices. (Step 2)
- Link to: Finance Policy, ARC Permanent Instructions 2024 and Legal Entity Management Tool (Umbrella) User Guide**

50 Statutory financial statements

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials

CONTROL & FREQUENCY

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

REQUIREMENTS

Audit fees negotiation and all additional audit related fees for all Group companies, and change of auditor at country level approvals are managed according to Group Delegated Authorities (GDA) and Approval of audit, audit-related and non-audit services Directive.

- A reconciliation between the financial statements per the Group reporting package and the statutory financial statements must be performed to ensure amounts are correct and complete. (Step 1)

• A reconciliation by flow of the equity between the Group reporting package and the statutory financial statements must be provided in Umbrella once the statutory financial statements are signed by the auditors based on a comprehensive template. (Step 1)

- Any adjustments made to the SAP Financial Consolidation (SAP-FC) financial reporting package (financial statements) to comply with the regulations of the statutory financial statements (e.g. International Financial

REQUIREMENTS

- Reporting Standards -IFRS- to a local Generally Accepted Accounting Principles -GAAP-, must be documented and approved by the CFO (or designee). (Step 1)
- The CFO (or designee) formally signs off on the statutory financial statements to confirm that they have been reviewed, and the amounts reported, including all relevant disclosures, are correct. (Step 1)
 - All statutory audits of a calendar year must be completed by April 30th of the following year. Any exceptions must be approved by the Group Head of Accounting, Reporting and Consolidation (ARC). Exceptions must be granted before the April 30th deadline, otherwise the MCS is not adequate. In the event of specific contractual constraints implied by commitments related to financing transactions and/or instruments (bonds, external debts, etc.) or other transactions requiring shorter timeline for the financial statements completion, the aforementioned due date of April 30th should be superseded by the applicable requirements for the related legal entities. The CFO (or designee) ensures that root causes of delays are analyzed and the organization and process are improved for the next year. (Step 2)
 - For both the statutory and group audits, a mandatory audit firm rotation is to take place every ten years, at the latest (more frequent intervals may be applied by the management). A previously appointed audit firm, after its rotation,

cannot be re-elected for a period of at least three years. Additionally, key audit partners must rotate every seven years, at the latest. A previously appointed key audit partner, after his/her rotation, cannot be re-elected, irrespectively of the audit firm in which he/she might work for. If local regulations of each country of incorporation dictate a more frequent mandatory rotation of audit firms or key audit partners and/or a longer waiting period for re-election, then local regulations supersede this guidance and the more frequent rotation periods and/or the longer waiting periods should be applied locally. Refer to the Approval of audit, audit-related and non-audit services Directive. (Step 2)

- All listed companies, at least seven days before the release of the statutory accounts, must: 1) provide a reconciliation of the equity, as well as the main indicators of the P&L, to the Group Head of ARC and the region CFO. This must be reviewed and confirmed by the Group Head of ARC and the region CFO; and 2) obtain formal approval by the Group Head of ARC and Group CFO, before any external publication of press releases including financial reporting but also all externally published reports. (Step 3)

Link to: Group Delegated Authorities, Finance Policy, Approval of audit, audit-related and non-audit services Directive, ARC Permanent Instructions 2024 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 & FREQUENCY

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

REQUIREMENTS

- At least quarterly, the country CFO (or designee) keeps track of and reviews the status of all uncertain tax positions, including: (Step 1)
 - the estimated maximum risk and estimated loss,
 - the classification as not probable, probable and virtually certain, and
 - the amount of the provisions recorded in the financial statements.
- Based on the information provided above, adjustments to provisions should be made accordingly, and contingencies must be appropriately disclosed. (Step 1)
- This detailed information is reported to Group Tax, using the format and tool communicated by Group Tax with all balances reconciled to SAP Financial Consolidation (SAP-FC). (Step 2)

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

52 Tax filings and payments

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

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

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

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

- A quarterly review of the deferred and current income tax calculations and related documentation is performed by the local Tax responsible and CFO (or designee), and includes: (Step 1)
 - appropriate representation on outstanding audits,
 - compliance with requirements of tax rulings,
 - enacted tax rate changes,
 - Tax Risks Provisions/Uncertain Tax Positions (UTPs) and exposures, including analysis of changes and or expirations, quantification, and probability assessment,
 - documented analysis of any temporary differences between the tax basis of an asset or a liability, and its carrying amount per the Statement of Financial Position, and proofs of all deferred tax balances,
 - reconciliation with amounts booked in the consolidation package,
 - tax rate reconciliation (prepared, documented, and validated),
 - recoverability of deferred tax assets is justified by supporting evidence, and
 - account reconciliation ending balances are verified to ensure all accounts requiring reconciliation are identified, and ending balances on the reconciliations are correct.
- Link to: Group Delegated Authorities, 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

All tax and legal rules regarding intercompany transfer prices and documentation are complied with; where required, transactions are reviewed by Group Tax. Any exceptions are discussed with Group Tax and 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 & FREQUENCY

1. **Confirmation by Group Tax and region Heads of Tax on the methodology used for intercompany transactions.** (Regional and Group level) *Annual*
2. **Approval by the Group Head of Tax on any exception to the Group Transfer Pricing Directive.** (Group level) *Annual*
3. **Review and analysis by the local Tax responsible and approval by the CFO (or designee) to check that the practice of the entity is in compliance with the Group Transfer Pricing Directive.** *Annual*
4. **Maintenance and filing, as applicable, by the local Tax responsible of the transfer pricing documentation in accordance with the local requirements and the Group Transfer Pricing Directive.** *Annual*

REQUIREMENTS

- The Transfer Pricing team with Group Tax together with the region Heads of Tax are accountable and responsible for analyzing, advising and confirming the transfer pricing methodology used in all intercompany transactions. (Step 1)
 - Any and all intercompany transactions must comply with the arm's-length principle as also required by local laws and regulation. (Step 1)
 - Any exceptions to the Group Transfer Pricing Directive should be discussed with Group Tax to evaluate the risk, and has to be formally approved by the Group Head of Tax. (Step 2)
 - The practice of the entity is regularly analyzed by the local Tax responsible and the CFO (or designee) to check compliance with the Group Transfer Pricing Directive. Risk analysis is communicated to the Finance and Legal departments to define potential needs for provisions or disclosures in accordance with the Minimum Control Standards (MCS) on tax risks. (Step 3)
 - Transfer pricing documentation is maintained and filed by the local Tax responsible. It shall be prepared with the assistance of the Transfer Pricing team 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

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

RISK

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

IMPACT

- Errors in financials
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

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

Link to: Finance Policy

Treasury



56 Bank relations

PRIMARY OBJECTIVE

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

RISK

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

IMPACT

- Compliance
- Financial losses
- Fraud

CONTROL & FREQUENCY

1. Obtain Group Treasury approval for any bank accounts that are opened, and notification of closing bank accounts to Group Treasury.

Upon request

2. Obtain Group Treasury approval for transactions with any counterparty that is not in the 'Bank List' prior to initiating transactions within approved limits. Monitoring of the credit exposure within the concentration limits published by Group Treasury. *Upon request*

3. Annual approval of the list of all bank accounts and optimization plan by the local CFO (or designee) based on the Treasury Directive, including inactive bank accounts analysis and timely closing, when applicable.

Annual

4. Quarterly verification by the local CFO (or designee) of the list of all open bank accounts reconciled with the Legal Entity Management tool (Umbrella) and the local treasury/accounting system. At least, yearly confirmation of authorized signatories obtained from banks to ensure it is consistent with the delegation of authority (DoA).

Quarterly

5. Identified counterparty risk exposure breaches must be reported to the Group Head of Treasury, and corrective actions implemented within the agreed time frame.

Upon change

REQUIREMENTS

- Bank relations, including fees, are approved as per the Group Delegated Authorities (GDA), when applicable, and Group Treasury Directive. (Step 1, 2)
- Any opening of bank accounts shall be approved by Group Treasury. Any closing of bank accounts shall be notified to Group Treasury, and updated in the Legal Entity Management tool (Umbrella). (Step 1)
- Information to the banks, including legal and compliance-related questions, needs to be provided in compliance with Group Treasury Directive. (Step 1)
- In order to limit credit exposure and concentration on any counterparty, the Group will only do business with authorized counterparties within concentration limits and guidelines described in the official Holcim Bank List. Within the Bank List, relationship banks should be considered over niche banks, unless niche banks offer a clear advantage. (Step 2)
- Business relationships with a bank not listed in the 'Bank List' are subject to written approval by the Group Head of Treasury. Any counterparty risk with non-relationship or non-niche banks must be under the limit defined through the approval process by Group Treasury. Request for approval (RfA) procedure and form includes sanctions screening as per the Group Treasury Directive. (Step 2)
- The country CFO (or designee) yearly reviews the list of active and inactive bank accounts, and ensures that the number of banks and bank accounts is optimized to increase visibility on cash and to reduce risks and costs. If it is not optimized, a plan is set up for closing accounts by a specific deadline. (Step 3)
- A local reconciliation of the approved bank accounts list with the Enterprise

Resource Planning (ERP) system and the Legal Entity Management tool (Umbrella) is to take place whenever a change occurs, or at least quarterly. Ensure that the Legal Entity Management tool (Umbrella) is up-to-date. (Step 3, 4)

• A process is in place to: (Step 4)
- ensure only joint signatory rights are allowed for any transaction with a bank, and each signatory has sufficient seniority to become an authorized signatory. Implement authorization limits for individual roles appropriate to the size of the organization.

- ensure immediate removal of signatory rights for employees no longer involved in the payment process, and inform the bank immediately in case of signatory changes, and

- obtain from the banks the list of authorized signatures to confirm it is up to date and consistent with the delegation of authority (at least once a year)

• Cash and deposit limits must be monitored. Any counterparty limit breach with non-relationship or non-niche banks shall be immediately reported, with the appropriate corrective actions, to the Head Group Treasury. Corrective actions are implemented within the time frame agreed with Group Treasury. (Step 5)

Link to: Group Delegated Authorities, Finance Policy, Treasury Directive, Sanctions and Export Controls Directive, Minimum Substance Requirements Directive, Counterparty Risk Management: Concentration limit applicable to countries, Holcim Bank List 2024 and Legal Entity Management Tool (Umbrella) User Guide

57 Cash transactions are not permitted without the 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 & FREQUENCY

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

REQUIREMENTS

- Cash transactions can create opportunities for fraud, money laundering and the funding of bribes. For this reason, the general rule is that cash transactions are not permitted. If the Group Head of Treasury and the Group Chief Compliance Officer approval is not formally granted, cash transactions are to be ceased. The following rules applies: (Step 1, 2)
 - maximum allowed petty cash limit per site is CHF 500, without need of an exception request. Petty cash is a small amount of cash kept on site to pay for minor expenses, such as office supplies or reimbursements, and also includes cash withdrawal options via corporate credit or debit cards,
 - supplier payments in cash are not allowed,
 - no cash collections are accepted from customers,
 - usage of checks is strongly discouraged and should be avoided. If used, only crossed checks are accepted (to be deposited to a bank account) for either supplier payment or customer receipt,
 - cash transactions to buy or sell foreign currencies at exchange offices (bureau de change) beside banks, are strictly prohibited. Countries which need to conduct such transactions must get approval from the Group Head of Treasury,
 - cash collections via mobile wallets shall be subject to Group Treasury and Group Compliance approval, and
 - Holcim countries which have been granted Group Head of Treasury and Group Chief Compliance Officer approval for cash transactions must perform restricted party screening on the third party (customer/supplier) in line with the Sanctions and Export Control Guidance.
- Validate with the region CFO, and obtain Group Head of Treasury and Group Chief Compliance Officer approval, for any exception to the requirements listed above, and inform Group CFO. If exceptions are approved, countries must implement a local procedure to: (Step 1, 2)
 - safeguard the process to issue and collect cash,
 - track, record and support with appropriate documentation, all approved cash and check transactions,
 - maintain segregation of duties between the person responsible for physical custody of cash/checkbook and the bank and cash disbursement authorized signatories. Restrict access to check books/cash and to the safe to only designated persons so as to ensure segregation of duties,
 - ensure an independent person who is not responsible for the physical custody of checks shall physically verify unused checks on hand and reconcile with the checkbook register on a quarterly basis. Random inventory counting has to be performed several times a year by an independent person, and
 - regularly perform (at least monthly) a reconciliation of checks and petty cash to the books, including petty cash used for employee advances. Investigate any variances within the same period, and confirm they are approved by the appropriate person before booking.

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

58 Secure payment means

PRIMARY OBJECTIVE

Payments are secured to avoid errors and safeguard assets

RISK

- Unsecured payment means 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 & FREQUENCY

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

REQUIREMENTS

For bank transfers:

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

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

58 Secure payment means

REQUIREMENTS

Business partner master data: (Step 4, 5)

- For entities that use treasury management applications or any other payment platforms, where Business Partners (i.e. banks, suppliers, entities, etc.) are created and maintained as master data, a master data management process that defines roles, responsibilities and rules is in place according to master data management guidelines as per MCS 29, and reviewed to ensure only authorized personnel can create, modify and delete financially relevant Business Partner data based on the required supporting documents (SSI, RIB, IBAN, etc.) and bank confirmation, as needed. Changes to bank information in the Treasury applications or in any other payment platforms must only be done post execution of the callback process using the registered contact information on file. The call must be documented with a post confirmation via email.

Direct debit (DD): (Step 6)

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

Link to: Finance Policy 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. Outstanding positions are reconciled with counterparty statements

.....

RISK

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

IMPACT

- Financial losses
- Errors in financials

CONTROL & FREQUENCY

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

59 Financial instruments, borrowings, commitments and working capital schemes

REQUIREMENTS

- Financial instruments, borrowings, commitments (e.g. trade finance facilities, surety bonds, guarantees lines, etc.), working capital schemes (e.g. supply chain financing, factoring, off balance sheet inventory financing), and related disbursements, can only be entered into after having been approved by appropriate personnel in accordance with local and Group Delegated Authorities and Group Treasury Directive. The Treasury Manager (or designated person) keeps track of all disbursements related to the repayment of borrowings, and ensures that both the repayments and the related borrowings are properly recorded, including the recognition of current and non-current portions of the liabilities. (Step 1)
 - Financing contracts have to be in line with the Holcim guide on loan documentation, any exception must be approved by Group Treasury. No financial covenants are accepted. Obtain Group Treasury approval for any financial contract not in line with the Holcim guide on loan documentation. (Step 1, 2)
 - The list of all financial instruments, borrowings, commitments and working capital schemes must be supported by adequate documentation and signed off by the CFO (or designee), as well as reported as per the reporting guidelines. (Step 3)
 - Third party and intercompany financing shall be renewed at least six months prior to maturity or earlier, if required. (Step 3)
 - Countries locally trading in derivatives due to regulatory reasons must quarterly reconcile the counterparties statements with the outstanding positions. Fair values are those indicated by Group Treasury. (Step 3)
 - Cash pool limits are approved by Group Treasury. Cash pool drawings must remain within approved limits. Any potential cash pool limit breach shall be immediately reported to the Head Group Treasury and remediated with appropriate corrective actions. Corrective actions are implemented within the time frame agreed with Group Treasury. (Step 4)
- Link to: Group Delegated Authorities, Finance Policy, Treasury Directive, 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 3.1.1.11. Description for Factoring of Trade Receivables reporting (Off / on balance sheet reporting), HARP 3.1.1.10 Off-balance Sheet Inventory Financing Arrangement, 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 are regularly reported and hedged according to the Group Treasury Directive

RISK

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

IMPACT

- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

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

Sustainability



61 Environmental impact

PRIMARY OBJECTIVE

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

RISK

- Air emissions (e.g. dust, Nox, Sox) exceeding authorized standards (Step 1)
- Excessive waste deposits and soil or water contamination (Step 1)
- Failure in quarry rehabilitation and biodiversity management (Step 1)
- Failure in water management (e.g. liquid effluents with detrimental impact on water resources) (Step 1)
- Deviation from CO₂ reduction standards (incl. internal Group targets) (Step 1)

IMPACT

- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

- All plants must have an environmental management system in place to ensure that all environmental impacts and risks are effectively managed and mitigated. Environment related permits (e.g. general environmental, emissions, water discharge, waste management) are to be reviewed annually to ensure compliance. (Step 1)
 - All sites must implement the HSE Critical Controls Management Pollution Priority Unwanted Event (PUE), with a quarterly verification review to be completed on iCare. (Step 1)
 - Environmental impacts have to be systematically identified according to the following steps: (Step 1)
 - identify environmental aspects of activities, products and services over which plants have control and/or influence,
 - assess the risks linked to the identified environmental aspects that may have a significant impact,
 - maintain an up-to-date catalog of significant environmental impacts during normal and abnormal operations.
 - Environmental impacts must be systematically managed to sustain and further improve environmental performance, while controlling environmental risks not only of our own operations, but including the supply chain. Progress must be monitored, evaluated and documented as required by the local regulations, or at least on an annual basis. (Step 1)
 - For cement plants, install and operate a continuous emission monitoring equipment for dust, nitrogen oxides (NOX), sulfur dioxide (SO₂), volatile organic compounds (VOC), and carbon monoxide (CO), as per the Holcim Emission Monitoring and Reporting standard. (Step 1)
 - Performance improvements on CO₂ emissions, water, circular economy and people must be aligned to commitments recorded in the CEM Plant Development Plans (PDP) and other environmental roadmaps, where applicable. (Step 1)
 - Water and waste must be managed preferring reuse and recycling to discharge and disposal, as per 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, at least yearly, environmental data and KPIs in the Sustainable Reporting Campaign according to the Holcim Environmental Reporting guidelines. (Step 1)
 - Monthly, Group Reporting Units (GRU) must report Sustainability KPIs according to Group ARC instructions. Inaccuracy or incompleteness of the KPIs in SAP-FC must be disclosed in the financial certification package. Sustainable Development indicators reported to the Group are based on validated data source, calculation method, and are reviewed for reasonableness, and validated by country Sustainable Development senior management on a half yearly basis. (Step 1)
- Link to: Health, Safety & Environmental Policy, Nature Policy, Climate Policy, Circular Economy Policy, Cement Environmental Directive, Water Directive, Quarry Rehabilitation and Biodiversity Directive, Sustainable Procurement Directive, Health, Safety & Environment Internally Generated Waste Standard, Health, Safety & 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

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

RISK

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

IMPACT

- Compliance
- Reputational damages
- Operational disruption
- Financial losses

CONTROL & FREQUENCY

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

REQUIREMENTS

All GRU must ensure that the following six elements of the Human Rights Approach are in place according to Human Rights and Social Policy and the Human Rights Directive:

- identify human rights risks and impacts: a Lead designated by the CEO conducts, at least every three years, a human rights assessment based on their risk level, covering our own operations, suppliers, business partners and communities, (Step 1)
 - address adverse impacts: all assessments (impact or self) must result in a Human Rights and Stakeholder Engagement Action Plan that must be reviewed at least annually. Major risks or impacts must be immediately added to the Action Plan, addressed by local Executive Committee (ExCo) and reported to the relevant Group function(s), (Step 1)
 - Grievance and remedy: a clear site-level mechanism (phone number, email address, etc.) for internal and external stakeholders to raise issues related to our operations exists and is managed by a function appointed by the entity ExCo. A record of all human rights-related complaints must be kept, and related follow-up actions are added in the Human Rights and Stakeholders Engagement Action Plan, (Step 2)
 - Stakeholder Engagement: every site must have a Stakeholder Map and a Human Rights and Stakeholder Engagement Action Plan managed at local level and updated at least annually. The Group Sustainability will approve the submitted Stakeholder Map and a Human Rights and Stakeholder Engagement Action Plan, as per the defined Group schedule. In cement plants and grinding units, a Community Advisory Panel (CAP) must be in place, (Step 3)
 - Monitor and communicate: results of the human rights assessments, an up-to-date version of the implementation of the Human Rights and Stakeholder Engagement Action Plans, and other key performance indicators (KPIs) defined by Group Sustainability must be reported via the Group reporting system annually, and (Step 4)
 - social initiatives are managed based on the local context and as per 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 and Sustainable Procurement 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 CO₂ reduction standards (incl. internal Group targets) (Step 1, 2, 3)

IMPACT

- Reputational damages
- Errors in financials

CONTROL & FREQUENCY

- 1. Climate country strategy: the country's climate-related initiatives, decarbonisation roadmap and any climate adaptation action plans related to EU Taxonomy are documented in the country strategy and Mid-Term Plan (MTP) process, and they shall be signed off by the Country CEO. *Annual***
- 2. CapEx plan: countries shall ensure that decarbonization-related actions (CapEx/OpEx) are clearly identified, classified and submitted in Group systems. *Annual***
- 3. Reporting: countries shall report monthly the climate-related KPIs according to Group ARC instructions after country Chief Sustainability Officer (CSO) validation. *Monthly***

REQUIREMENTS

Strategy: (Step 1)

- Group companies shall include details of their climate-related strategies (short, medium and long term) as part of the country strategies, and shall elaborate details of the decarbonization roadmap (Scope 1 and 2) in the Mid-Term Plan (MTP),
- country targets shall be consistent with the Group decarbonization ambition, with confirmation that the consolidation of all country decarbonization roadmaps reflects Group targets,
- for decarbonization projects requiring the use, generation, or purchase of carbon credits, the business case prepared by the country CSO (or designee) for Carbon Credit Office approval shall be validated by the country CEO, and
- climate adaptation measures shall be taken into consideration to align with the EU-Taxonomy 'Do No Significant Harm' criteria (DNSH) on climate change adaptation, and shall be documented in the iCare tool.

CapEx Plan: (Step 2)

- annually, the country CSO (or designee) and the country CFO shall ensure that resource allocation (CapEx/OpEx) for climate-related projects or actions is incorporated into the country's Mid-Term Plan (MTP) and reconciles with the CEM Plant Development Plans (PDP), and
- Green CapEx, based on HARP definition, shall be consistently reflected in the CapEx reporting in One PPM (where applicable), and in SAP-Financial Consolidation (SAP-FC).

Reporting: (Step 3)

- monthly, the country CSO (or designee) shall validate the climate-related financial and non-financial indicators reported to the Group,
- annually, the climate-related indicators reported to the Group shall be based on validated data source, calculation method, and shall be reviewed for accuracy and validated by the country CSO (or designee),
- carbon credit-related KPIs shall be reported to the Group by the Project Lead, with the validation by the country CSO, for the annual reporting campaign, and
- inaccuracy or incompleteness of the KPIs in SAP-Financial Consolidation (SAP-FC) must be disclosed to the financial certification package.

Link to: Nature Policy, Climate Policy, Circular Economy Policy, Quarry Rehabilitation and Biodiversity Directive, Sustainable Procurement Framework (Environment and Sustainability), Holcim Environment Questionnaire, Holcim Sustainable Constructions Questionnaire, Scope 3 Standard, Carbon Credit Directive, HARP 3.1.8.4 Green CAPEX, HARP 6.2.3 Sustainable Development - CO₂ and HARP 7.3.7 Taxonomy Reporting

Operational Technology (OT)



64 OT security baseline controls for cement plants and grinding stations

PRIMARY OBJECTIVE

Reduce the risk of cyber attack on the cement plant's and grinding station's OT systems

RISK

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

IMPACT

- Operational disruption
- Reputational damages
- Financial Losses
- Fraud

CONTROL & FREQUENCY

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

REQUIREMENTS

Note: Operational Technology (OT) systems refers collectively to cement plant's and grinding station's industrial applications and OT infrastructure (hardware, operating system, database, network, interfaces)

The detailed step wise requirements for this MCS are defined in the Minimal Control Standards for Operations Technology (OT) which are applicable for each of the defined controls. Full compliance is required against each of the requirements.

- OT security organisation and governance is established. Regular OT security trainings are conducted. Basic cyber incident response plan is implemented. (Step 1)

- OT asset inventory and basic lifecycle management is in place. (Step 2)
- Separation of OT network from IT using firewalls and segmentation within the OT network. (Step 3)
- Secured logical access environment (including remote) is established. (Step 4)
- Basic endpoint protection systems on the endpoints is installed (Antivirus/EDR). (Step 5)
- Critical OT systems backup and restore procedures are documented and implemented. (Step 6)
- OT server rooms meet secured access and environmental controls. (Step 7)

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

Acronyms

Accounting, Reporting and Consolidation (ARC)	Capital expenditures (CAPEX)	Chief Sustainability Officer (CSO)
Directors & Officers (D&O)	Generally Accepted Accounting Principles (GAAP)	Group Treasury i/o Corporate Finance and Treasury (CFT)
Information Technology (IT)	Manual Journal Entries (MJE)	People on Board (POB)
Request for Proposal (RfP)	Security & Resilience Management System (SRMS)	Terrorist & Organised Crime (TOC)
Anti-Bribery and Corruption (ABC)	Cash-Generating Unit (CGU)	Country Security Representative (CSR)
Do Not Significant Harm (DNSH)	Group Delegated Authorities (GDA)	Holcim Front-End Reporting Tool (Hive)
Information Technology Service Centers (ITSCs)	Mid-Term Plan (MTP)	Personally identifiable information (PII)
Risk with zero conflicts (RWZC)	Security Incident Notification Tool (SINT)	Third Party Due Diligence (TPDD)
Biodiversity Indicator and Reporting System (BIRS)	Change in structure (CIS)	Data Universal Numbering System (DUNS)
Enterprise Resource Planning (ERP)	Group Insurance and Risk Financing (GIRF)	Holcim Accounting and Reporting Principles (HARP)
International Financial Reporting Standards (IFRS)	Minimum Control Standards (MCS)	Property Damage / Business Interruption (PDBI)
SAP Bank Communication Manager (SAP-BCM)	Security Services with Integrity (SSI)	Third Party Liability (TPL)
Board of Directors (BoD)	Conflict of Interests (COI)	Delegation of authority (DoA)
Environmental, social, and governance (ESG)	Group Level Material Risks (GLMRs)	Health, Safety and Environment (HSE)
International Organization for Standardization (ISOs)	Operating expenses (OPEX)	Property, Plant and Equipment (PPE)
SAP Flexible Real Estate Management (RE-FX)	Segregation of Duties (SoD)	Uncertain Tax Positions (UTPs)
SAP Flexible Real Estate Management (RE-FX)	Construction in Progress (CIP)	Direct Debit (DD)
Business Resilience Team (BRT)	Group Reporting Unit (GRU)	Health, Safety & Environment Improvement Plan (HSEIP)
Expected Credit Loss Model (ECL)	Operational Technology (OT)	Resilience and Governance (RaG)
Key Performance Indicators (KPIs)	Senior Leaders Group (SLG)	Value Added Tax (VAT)
SAP Governance, Risk, and Compliance (SAP-GRC)	Country Chief Executive Officer (CCEO)	
Business Service Centers (BSCs)	Group Risk Insurance Tool (GRIT)	
Foreign Exchange (FOREX or FX)	Pension and Benefits Governance Team (PBG)	
Legal Entity Management Tool (Umbrella)	Sites Mapping Application (SMA)	
SAP- Financial Consolidation (SAP-FC)		



Holcim Ltd.

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

Cover photo:
Fabryka Norblina (Norblin Factory),
Warsaw, Poland. The renovation
of the Norblin Factory into a lively
retail and gastronomic zone in
Warsaw used Hydromedia concrete
to create an ecological and
effective drainage substructure.