

# Enterprise Risk Management

## Developing Risk Categories That Support Risk Assessment

# Risk Assessment Approach

- **Identifying Specific Regulatory Frameworks**
  - A separate risk categorization focused on external regulatory frameworks (authoritative sources) should then be developed to support discussions about compliance expectations.
    - Each regulatory area should have a risk owner assigned to oversight risk and control mitigation for that authoritative source across the organization.
- **Compliance in the Context of Enterprise Risks**
  - SunHawk has seen successful organizations create a view of their Enterprise Risk Categories at a high level to bring context to where the categories of risk align to the organization strategy and operations.
    - Mitigation initiatives for strategic, operational, financial and compliance risks need to be embedded into the organization.
    - Compliance cannot be seen as a separate activity from operations and corporate function activities.

# Enterprise Risk Management – Risk Framework Categories

A risk framework is used by leadership teams, departments, process owners, and division leaders to proactively brainstorm specific risks to the achievement of objectives. Resources and time should then be prioritized to appropriately mitigate those specific risks.

Strategic Risks	Operational Risks	Financial Risks	Compliance Risks
<p><b>Planning Risks:</b></p> <ul style="list-style-type: none"> <li>• Strategic Planning &amp; Forecasting</li> <li>• Business Portfolio Change</li> <li>• Competitor Actions</li> <li>• Economic Conditions</li> <li>• Industry Consolidation</li> <li>• Industry Disruption</li> <li>• Global, Macro &amp; Micro Trends                             <ul style="list-style-type: none"> <li>• Social</li> <li>• Technological</li> <li>• Economic</li> <li>• Environmental</li> <li>• Political</li> </ul> </li> </ul> <p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• Leadership &amp; Succession Planning</li> <li>• Organizational Design</li> <li>• Authority &amp; Limits</li> <li>• Product Development Lifecycle</li> <li>• Stakeholder Relations</li> <li>• Brand &amp; Reputation Management</li> <li>• Social Responsibility</li> </ul>	<p><b>Planning Risks:</b></p> <ul style="list-style-type: none"> <li>• Operational Planning &amp; Forecasting</li> <li>• Innovation, Continuous Improvement, &amp; Learning</li> <li>• Insights, Data Analytics, &amp; Consumer Research</li> <li>• Client Satisfaction, Provider Satisfaction &amp; Perfect Service</li> <li>• Product Safety &amp; Liability</li> </ul> <p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• Perfect Service Culture</li> <li>• Account Management</li> <li>• Intellectual Property</li> <li>• Process Management</li> <li>• Technology Management</li> <li>• Vendor Management</li> <li>• Facilities Management</li> <li>• Human Resources Management</li> <li>• Supply Chain Management</li> <li>• Sales Inventory Management</li> <li>• Sales Channel Prospecting &amp; Sales Execution</li> <li>• Associate Health &amp; Safety</li> <li>• Product Safety</li> <li>• Business Interruption</li> <li>• Fraud, Waste &amp; Abuse</li> <li>• Acquisition Integration</li> </ul>	<p><b>Planning Risks:</b></p> <ul style="list-style-type: none"> <li>• Financial Planning &amp; Forecasting</li> <li>• Working Capital Forecasting &amp; Management</li> <li>• Sales Pipeline Forecasting</li> <li>• Capital Availability</li> <li>• Lending Covenants</li> <li>• Investor Goals</li> </ul> <p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• Capital Allocation &amp; Resource Prioritization</li> <li>• Pricing and Underwriting</li> <li>• Administrative Cost Containment</li> <li>• Financial Reporting Accuracy</li> <li>• Accounts Receivable and Payable Management</li> </ul>	<p><b>Planning Risks:</b></p> <ul style="list-style-type: none"> <li>• Regulatory Forecasting</li> </ul> <p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• Ethical Conduct</li> <li>• Securities Regulations</li> <li>• Regulatory Filings – Financial</li> <li>• Construction Regulations</li> <li>• Information Security</li> <li>• Privacy Regulations</li> <li>• Contract Adherence</li> <li>• Litigation</li> <li>• Advertising Laws</li> <li>• OSHA / Employee Regulations</li> <li>• Fraud Prevention</li> </ul>

# Example Compliance Risk Categories

A compliance risk framework is used by leadership teams, departments, process owners, and division leaders to proactively brainstorm specific compliance risks at a greater level of detail to the enterprise risk framework. Resources and time should then be prioritized – in relation to overall risks and appetite - to appropriately mitigate specific compliance risks.

General Compliance Risks	Mortgage Compliance Risks	Retail Risks	Corporate Compliance Risks
<p><b>Planning Risks:</b></p> <ul style="list-style-type: none"> <li>• Compliance Leadership &amp; Succession Planning</li> <li>• Regulatory Forecasting                             <ul style="list-style-type: none"> <li>• State Regulators</li> <li>• Federal Regulatory</li> <li>• Non-US Regulatory</li> </ul> </li> </ul> <p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• Compliance Staffing</li> <li>• Compliance Organizational Design and Accountability Assignment</li> <li>• Compliance Reporting</li> <li>• Compliance Risk Assessment</li> <li>• Fraud, Waste &amp; Abuse Assessment</li> <li>• Ethical Conduct</li> </ul>	<p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• Anti-Money Laundering</li> <li>• Equal Credit Opportunity Act</li> <li>• Fair Credit Reporting Act</li> <li>• Fair Debt Collection Practice Act</li> <li>• Fair Housing Act</li> <li>• Privacy of Consumer Financial Information</li> <li>• Truth in Lending Act</li> <li>• Real Estate Settlement Procedures Act (RESPA)</li> <li>• Secure and Fair Enforcement for Mortgage Licensing</li> <li>• Unfair, Deceptive, or Abusive Acts or Practices</li> <li>• Telephone Consumers Protection Act</li> <li>• Homeowner Protection Act</li> <li>• Service Members Civil Relief Act</li> <li>• Fair and Accurate Credit Transactions Act</li> <li>• EFT</li> <li>• Loan Originator Compensation Rule</li> <li>• FTC Advertising Rules</li> <li>• E-sign Act</li> <li>• OFAC Compliance</li> <li>• IRS 1098 requirements</li> <li>• PCI – Debit/Credit Card Security</li> <li>• Foreclosure requirements—state statutes</li> <li>• Bankruptcy Code</li> <li>• Government Loan Annual Renewal (FHA, VA, RHS)</li> <li>• Loan file retention policy</li> <li>• CFPB                             <ul style="list-style-type: none"> <li>• Vendor management</li> <li>• Customer Complaint Process</li> </ul> </li> </ul>	<p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• HUD                             <ul style="list-style-type: none"> <li>• State Requirements</li> </ul> </li> <li>• Licensing of Contractors</li> <li>• Information Security / PCI</li> <li>• Licenses                             <ul style="list-style-type: none"> <li>• Annual renewal</li> <li>• State issue</li> <li>• Salespeople license</li> </ul> </li> </ul> <p><b>Insurance Product Risks</b></p> <p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• Department of Insurance                             <ul style="list-style-type: none"> <li>• Statutory Reporting</li> </ul> </li> <li>• State Policy Changes</li> <li>• Agent licensing (State) / State Licensing</li> </ul>	<p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• Securities Regulations &amp; Filings                             <ul style="list-style-type: none"> <li>• 10K / 10Q</li> <li>• Form 4</li> <li>• Section 16 filers</li> <li>• Disclosures</li> </ul> </li> <li>• NASDAQ regulatory guidelines</li> <li>• Investor Communication / Fair Disclosure</li> <li>• Tax filings (federal, state, local)</li> <li>• Conflict Minerals (Form SD)</li> <li>• Dodd-Frank reporting</li> <li>• Census reporting</li> <li>• Information Security</li> <li>• Privacy Regulations                             <ul style="list-style-type: none"> <li>• HIPAA, GDPR</li> </ul> </li> <li>• Contract Adherence</li> <li>• Contract management</li> <li>• Intellectual Property</li> <li>• Litigation Management</li> <li>• Government Procurement</li> <li>• Advertising Laws</li> <li>• Human Resources                             <ul style="list-style-type: none"> <li>• DOL Requirements</li> <li>• FLSA</li> <li>• Minimum Wage</li> <li>• Hiring Discrimination</li> </ul> </li> </ul>
<p><b>Manufacturing Compliance Risks</b></p> <p><b>Execution Risks:</b></p> <ul style="list-style-type: none"> <li>• HUD</li> <li>• OSHA</li> <li>• EPA</li> <li>• State code compliance</li> <li>• Licensing                             <ul style="list-style-type: none"> <li>• Plant</li> <li>• Retailers</li> <li>• Salespeople</li> </ul> </li> </ul>			