Zava Corporation Legal Governance and Compliance Framework

Introduction:
Zava Corporation, a U.S.-based retail company, has established a comprehensive legal governance framework to ensure ethical leadership, strict regulatory compliance, financial integrity, and robust risk management. This document outlines Zava's corporate governance structure, key policies, and controls across all facets of legal governance, including corporate oversight, compliance with U.S. laws and regulations, financial reporting and audits, data governance and privacy, payment security, Sarbanes-Oxley (SOX) and other statutory obligations, ethical conduct standards, and internal control processes. The framework is designed in a formal, professional manner consistent with real-world corporate governance, and can serve as a model for building legal-focused AI agents. It provides clarity on roles and responsibilities, describes policies and procedures, and explains how Zava meets its legal and ethical obligations. All sections prioritize core principles first, followed by detailed requirements and context.

Corporate Governance Structure and Responsibilities

Board of Directors: Zava's corporate governance begins with its Board of Directors, which provides **strategic direction and oversight**. The Board is responsible for high-level governance matters such as overseeing enterprise risk management, setting the company's long-term strategy, ensuring legal and regulatory compliance, and monitoring overall performance . The Board operates independently of day-to-day management and focuses on policies and objectives rather than operational decisions . Key duties of the Board include approving corporate policies, major initiatives, and financial plans; selecting and evaluating the CEO and executive leadership; and ensuring that the company meets its obligations to shareholders and stakeholders. In alignment with best practices of corporate governance, there is a **clear separation of duties** between the Board and management to maintain checks and balances .

Executive Management: The **management team**, led by the Chief Executive Officer (CEO), is responsible for executing the Board's strategy and handling Zava's daily operations. The CEO reports to the Board and is accountable for implementing Board decisions and upholding the governance standards set by the Board. Supporting the CEO are other C-suite executives such as the Chief Financial Officer (CFO), Chief Operating Officer (COO), and, in Zava's case, a Chief Legal/Compliance Officer (or General Counsel) given the emphasis on legal governance. The **CFO** manages financial strategy, accounting, and reporting, ensuring that financial records are accurate and controls are effective. The CFO also presents financial results to the Board and shareholders, and certifies financial statements as required

(particularly under Sarbanes-Oxley). The **Chief Legal/Compliance Officer** (or General Counsel) oversees the company's legal affairs and compliance program, advising the Board and management on legal risks, and ensuring that internal policies meet regulatory standards. Zava's **COO** oversees retail operations (sales, supply chain, etc.), focusing on operational efficiency and execution of business plans.

Board Committees: To strengthen oversight, the Board delegates certain functions to specialized committees: most critically an **Audit Committee** is established to oversee financial reporting, audits, and compliance. The Audit Committee (comprised of independent directors) supervises the external auditor relationship and internal audit function, reviews financial statements, and ensures that robust internal controls are in place. It also pre-approves any non-audit services provided by the external auditor to safeguard auditor independence. In addition, Zava's Board may form other committees, such as a Risk and Compliance Committee (overseeing enterprise risk management and legal compliance issues) and a Nominating and Governance Committee (overseeing board governance practices and ethics). These committees regularly report back to the full Board, ensuring that each governance aspect (audit, risk, ethics, etc.) receives focused attention.

Below is a summary of key roles in Zava's governance structure and their core responsibilities:

(Note: Titles and roles may overlap; for instance, Zava's General Counsel may serve as Chief Compliance Officer. The key principle is clear assignment of responsibility for each governance domain.)

This governance structure ensures that **accountability** is maintained at the highest level. The Board (particularly through its committees) holds management accountable for operating within the established ethical and legal boundaries, and **management** in turn maintains accountability down through all levels of the company. Shareholders and stakeholders can have confidence that Zava's leadership is directing the company with proper oversight mechanisms in place, consistent with U.S. corporate governance best practices .

Ethical Conduct and Code of Professional Conduct

A cornerstone of Zava's governance is a strong culture of **ethics and integrity**. Zava has adopted a comprehensive **Code of Professional Conduct** that applies to all employees, officers, and directors. This Code sets forth clear expectations for ethical behavior, professional integrity, and compliance with the law in every aspect of the company's operations. Senior leadership, including the CEO and CFO, are not only subject to the Code but are also charged with setting the "tone at the top" by demonstrating unwavering commitment to ethical standards and enforcing those standards throughout the organization .

Key Principles of the Code: Zava's Code of Conduct emphasizes:

- **Honesty and Integrity:** All personnel must conduct business honestly and transparently, avoiding conflicts of interest and never misrepresenting facts or engaging in fraudulent behavior .
- **Compliance with Laws:** Employees are required to know and follow all applicable laws and regulations at the local, state, and federal levels, as well as industry-specific regulations that apply to Zava's retail operations. This includes securities laws, consumer protection laws, anti-bribery laws, employment laws, and any other regulations relevant to the company's activities.
- **Accuracy and Transparency:** All financial records, reports, communications, and disclosures must be accurate, complete, timely, and understandable. No one at Zava shall falsify records or conceal truthful information. This principle ties directly into the company's financial reporting obligations (discussed later) and is essential for maintaining trust with stakeholders.
- **Confidentiality and Data Protection:** Employees must safeguard confidential information, including customer data, proprietary business information, and personal data of employees. Such information is only to be used for legitimate business purposes and disclosed only when authorized or legally required . (Zava's data governance and privacy policies, described further below, support this principle.)
- **Responsible Use of Assets:** All company assets and resources (financial assets, physical property, digital assets, etc.) are to be used responsibly and solely for the benefit of the company and its stakeholders, not for personal gain .
- **Professional Excellence and Diligence:** Employees and especially members of the finance and legal teams are expected to perform their duties with diligence, competence, and good judgment. They should continually improve their skills and share knowledge to benefit the organization and its stakeholders .
- **Reporting and Non-Retaliation:** Zava strongly encourages reporting of any suspected misconduct, violations of the Code, or legal concerns. Multiple channels are available for raising concerns (e.g., reporting to a supervisor, a compliance hotline, or the compliance team), and reports can be made confidentially or even anonymously. The Code and company policy strictly prohibit retaliation against anyone who reports in good faith . All reports are treated with discretion and appropriately investigated.
- **Accountability and Enforcement:** Adherence to the Code of Conduct is a condition of employment. Violations of the Code or other company policies result in disciplinary action, up to and including termination of employment . Senior executives who violate the Code may also face removal and possible legal consequences. The Board (often through the Audit or Ethics Committee) receives

reports on significant Code violations and how they were addressed, ensuring top-level oversight of corporate integrity.

These ethical principles are **ingrained in training programs** and communications across Zava. All employees must complete periodic ethics and compliance training to refresh their understanding of the Code and relevant laws. New hires receive Code of Conduct training as part of onboarding. Managers have a special responsibility to not only follow the Code themselves but also to ensure their teams understand and live up to the company's standards.

By cultivating an environment where ethical conduct is the norm and expected, Zava protects its reputation, builds trust with customers and partners, and reduces the risk of legal or regulatory violations. The strong ethical culture also complements the other elements of governance (such as compliance and internal controls) by encouraging employees to speak up about issues before they become serious problems.

Legal and Regulatory Compliance Program (U.S. Jurisdiction)

Zava operates in a heavily regulated environment (as all retail businesses do) and has implemented a **robust compliance program** to ensure full adherence to all applicable laws and regulations in the United States. This program is overseen by the Chief Compliance Officer (or General Counsel) and the Board's Risk/Compliance Committee, and it spans multiple domains of law, reflecting the diverse obligations of a U.S.-based retailer. Key features of the compliance program include:

- **Identification of Applicable Laws:** Zava continuously identifies and monitors the laws and regulations that apply to its business. This includes corporate and securities laws (since Zava is presumably a public company), consumer protection laws (governing advertising, product safety, fair pricing, etc.), data privacy and protection laws (discussed in Data Governance below), labor and employment laws (wages, workplace safety, non-discrimination, etc.), environmental regulations (for any environmental impact of retail operations or supply chain), anti-trust/competition laws, and industry-specific guidelines (such as Federal Trade Commission rules for retail promotions and e-commerce). A comprehensive registry of these requirements is maintained by the compliance team.
- **Policies and Procedures:** For each major compliance area, Zava has internal policies and procedures to guide employees. For example, there are policies on truthful advertising and marketing practices to comply with FTC regulations, product safety and recall procedures to comply with Consumer Product Safety Commission (CPSC) standards, and protocols for handling customer data in line with privacy laws. These policies translate legal requirements into clear do's and don'ts for staff.
- **Training and Awareness:** Regular training sessions are conducted to ensure employees understand relevant regulations and how to comply. For instance, store

managers and marketing teams receive training on consumer protection and advertising law; HR and management receive training on employment law and anti-harassment; IT and customer service teams are trained on data privacy requirements. The goal is to embed compliance awareness in daily operations.

- **Monitoring and Auditing:** Zava's compliance program includes ongoing monitoring of business activities and periodic audits to check that policies are followed. This could involve routine inspections of retail operations, audits of financial transactions (to ensure no violations like money laundering or sanctions violations), or reviews of data practices. Internal Audit and the compliance team work together to test compliance controls and identify any gaps.
- **Reporting and Issue Management:** If a compliance issue or potential violation is identified, either through audits, employee reports, or regulatory inquiries, Zava has a process to investigate and remediate. Issues are documented, root causes analyzed, and corrective actions implemented. Serious compliance issues are escalated to senior management and the Board. The company also self-reports to regulators and cooperates as required by law.
- **Regulatory Engagement:** Zava maintains open communication with regulators and stays current on regulatory changes. The compliance team (and legal counsel) reviews new laws or rule changes (for example, changes in state privacy laws or labor laws) and updates company policies accordingly. They also ensure timely filing of any required reports to regulators.

Importantly, Zava's legal compliance efforts are not just about following the letter of the law, but also aligning with the **spirit of good governance**. In other words, beyond mandatory regulations, Zava strives to uphold high standards of corporate citizenship and ethical conduct. This proactive stance helps prevent legal issues and positions the company as a trustworthy retailer.

The Board's oversight ensures that compliance is taken seriously at all levels. Regular reports on compliance status are provided to the Board (e.g., summary of training completed, audit findings, any regulatory fines or investigations, etc.). This top-down support empowers the compliance function to enforce policies without undue pushback.

Zava's compliance with legal requirements is **comprehensive**: the company endeavors to meet **all relevant U.S. laws and regulations** that apply to its operations and products. This broad compliance mandate falls under the purview of corporate governance as well. A healthy governance program, like Zava's, integrates compliance into the corporate governance framework to ensure the company acts lawfully and ethically in all respects.

Financial Reporting, Auditing, and SOX Compliance

Financial integrity is a critical part of Zava's governance. As a retail company operating in the U.S., Zava must adhere to Generally Accepted Accounting Principles (US GAAP) in its

accounting, and if it is publicly traded, it must also comply with the rules of the U.S. Securities and Exchange Commission (SEC) for financial reporting. The company has instituted rigorous policies and controls to ensure that its financial statements are accurate, timely, and compliant with all applicable standards, and that it maintains effective internal control over financial reporting. Additionally, Zava is committed to full **Sarbanes-Oxley Act (SOX)** compliance, given its importance for U.S. public companies in preventing fraud and protecting investors.

External Financial Reporting & Audit Practices

Zava prepares **quarterly and annual financial statements** (e.g., 10-Q quarterly reports and 10-K annual reports if it's an SEC registrant) that fairly present the company's financial condition and operating results in all material respects. These reports are compiled in accordance with US GAAP and SEC regulations. Key aspects include:

- **Accuracy and Completeness:** Financial statements and disclosures must be free of material misstatements or omissions. Zava's policy is that all transactions are recorded properly and that any accounting estimates are made in line with applicable accounting standards. Off-balance sheet arrangements or obligations are disclosed fully to avoid any misunderstanding of the company's financial position.
- **Management Certification:** Under SOX Section 302, the CEO and CFO must certify each quarterly and annual report, attesting to the accuracy of financial statements and to the effectiveness of disclosure controls and procedures. Zava's CEO and CFO formally certify that they are responsible for internal controls and that they have disclosed any significant deficiencies or fraud to the auditors and Audit Committee.
- **Internal Control Report:** Under SOX Section 404, Zava includes in its annual 10-K a report on internal control over financial reporting, acknowledging management's responsibility for controls and presenting an assessment of their effectiveness. The external auditor also provides an attestation on the effectiveness of internal controls over financial reporting as part of the integrated audit.
- **Independent External Audit:** Zava engages an independent registered public accounting firm (external auditor) to audit its annual financial statements and internal controls. The **external auditor** provides an unbiased examination of Zava's books and records and issues an audit opinion published in the annual report. To ensure the auditor's independence, Zava strictly controls the other services (if any) that the auditor may provide. In line with SEC rules and company policy, the Audit Committee pre-approves **all audit and non-audit services** from the audit firm. Certain non-audit services that could pose conflicts (like financial systems consulting) are prohibited outright. The Audit Committee also reviews the auditor's performance and rotates the lead audit partner as required by law.
- **Audit Committee Oversight:** The Audit Committee of the Board plays a central role in external financial reporting. They review draft financial statements and earnings

releases, confer with management and auditors about significant reporting issues or judgments, and ensure that **appropriate accounting policies** are in place. The committee also monitors the resolution of any audit findings. Zava's Audit Committee includes members with financial expertise (such as former finance executives) to effectively oversee this process, as required by stock exchange rules.

- **External Reporting Governance Policy:** Zava's approach mirrors the structure of its holding company external financial reporting governance framework in that Corporate Accounting (or in Zava's case, the Finance department under the CFO) manages a company-wide framework to uphold the integrity of financial reports . Any policies or procedures outside the finance function that impact financial reporting must also comply with Finance's standards and U.S. GAAP. For example, if the Sales or Operations department has a policy that affects revenue recognition or inventory accounting, it must be in line with corporate accounting policies and approved by Finance to ensure consistency and compliance.
- **Fiduciary Responsibility:** Zava's CFO and Controller (Chief Accounting Officer) have fiduciary duties to maintain accurate accounts and sound financial processes. This includes ensuring that **financial systems changes** are controlled. Zava has adopted a change-management policy for financial systems similar to its holding company, which requires that any changes to core financial IT systems (like general ledger software or payment systems) be reviewed and approved by appropriate senior finance leaders to prevent unintended impacts on financial data integrity.

Through these measures, Zava fulfills the requirements of U.S. financial regulation and instills confidence in its investors and stakeholders that the financial information released is reliable. If Zava is subject to SEC jurisdiction, it will timely file all required reports (10-K, 10-Q, 8-K for significant events, proxy statements, etc.) and comply with SEC regulations like Regulation FD (Fair Disclosure) for communications.

Additionally, **statutory financial compliance** is ensured not just at the consolidated level but in every jurisdiction where Zava operates. For example, if Zava has any subsidiaries or operations in specific U.S. states or foreign countries that require separate financial statements or statutory filings, Zava will comply with those local GAAP and audit requirements as well. In our holding company policy, even where a formal local law requirement doesn't exist, they prepare local financials and go through internal review and approval to maintain discipline. Zava likewise commits to meeting all legal obligations for financial reporting, whether federal or state, and will undergo any required audits (or seek approved exceptions only when appropriate and lawful) to remain in good standing with regulatory bodies.

Internal Controls and SOX Compliance

Zava maintains a robust system of **internal controls over financial reporting and operations** to ensure that all financial transactions are recorded correctly and that the risk of fraud or

error is minimized. This internal control framework aligns with the COSO model (Committee of Sponsoring Organizations of the Treadway Commission) and addresses the control environment, risk assessment, control activities, information & communication, and monitoring activities. Key components include:

- **Control Environment:** As described under Ethical Conduct, Zava's leadership fosters an ethical environment that supports good controls. There is clear organizational structure, assignment of authority, and competent staff in financial roles, which together lay the foundation for effective internal control.
- **Risk Assessment:** Management regularly evaluates financial reporting risks (e.g., risk of misstating revenues, risk of theft of assets, risk of improper valuation of inventory, etc.) and designs controls to address these risks. The Audit Committee and Board are involved in understanding and approving the approach to risk management in financial reporting.
- **Control Activities:** These are the actual policies and procedures put in place to address financial risks. Zava has documented dozens of controls throughout its processes. Particularly important are the controls around **accounting processes and period-end financial close**, which ensure completeness and accuracy of the books each period. The next subsection details certain key financial control policies (account reconciliations, journal entries, closing process) that Zava employs. Other examples of control activities include requiring dual approvals on expenditures, segregation of duties (so that no single individual can authorize, execute, and record a transaction unchecked), system access controls, and automated validations in IT systems (for instance, preventing an accounting entry that doesn't balance).
- **Information and Communication:** Zava ensures that pertinent financial information is identified, captured, and communicated in a form and timeframe that enable personnel to carry out their responsibilities. The policies and expectations for internal controls are documented and communicated through manuals and training. There are also clear channels for reporting issues upward (for example, an employee can escalate a control concern to management or Internal Audit).
- **Monitoring:** The internal control system is regularly monitored through self-assessments and independent evaluations. Zava has an **Internal Audit** department that conducts audits of various processes on a rotating basis to test the effectiveness of controls, including those related to financial reporting and compliance. They report their findings to the Audit Committee. Also, as part of SOX compliance, management and the external auditors annually evaluate the effectiveness of internal controls over financial reporting, as noted. Any identified weaknesses (deficiencies) are remediated promptly.

Under **Sarbanes-Oxley Act compliance**, Zava's program focuses on fulfilling both Section 404 (internal control assessment) and Section 302 (officer certifications) requirements. In

practice this means Zava has a SOX compliance team that coordinates documentation of controls, testing of controls, and remediation of any issues, working closely with Internal Audit. Each year, key control owners in finance and other departments certify the effectiveness of their controls up the chain, culminating in the CEO/CFO certification mentioned earlier. By doing so, Zava has effectively "established a corporate governance structure that enforces compliance with SOX" just as our holding company and other companies are required to do. The outcome is that Zava's leadership can confidently assert (and demonstrate via audit evidence) that the financial reports are accurate and that any material weaknesses in controls would be detected and addressed.

Moreover, compliance with SOX has ancillary benefits: it forces discipline in financial processes and deters fraud. SOX also requires that Zava has mechanisms for employees to report concerns about accounting or auditing (often called a whistleblower hotline). As noted in the Ethics section, those mechanisms are in place and are administered in a way that protects whistleblowers, fulfilling SOX mandated protections.

Key Financial Control Policies and Procedures

To operationalize its internal control framework, Zava has specific policies governing critical accounting processes. These policies ensure consistency, accountability, and compliance in the finance function and serve as **baseline controls** for accurate financial reporting. Below are key financial control policies, inspired by the provided holding company policy templates but tailored for Zava's needs:

Policy	Purpose & Scope	Key Requirements
Account Reconciliation Policy	Ensure all balance sheet accounts are correct and supported. Covers how and when account reconciliations must be performed for all general ledger accounts.	– **Frequency:** All active balance sheet accounts must be reconciled at least quarterly; high-risk or key accounts (as identified by Finance) are reconciled monthly. – **Responsibility:** Each account is assigned an owner (Preparer) responsible for reconciling, a Reviewer, and an Approver in a controllership role. – **Supporting Documentation:** Reconciliations include supporting schedules or documents, retained in the designated reconciliation system or repository. – **Timeliness:** Reconciliations and reviews/approvals must be completed within defined deadlines after period close (e.g., within 30 days of quarter-end). – **Follow-up:** Any discrepancies or unreconciled differences are investigated and resolved promptly; issues are escalated if they indicate potential errors or irregularities.

Journal Entry Management Policy	Maintain integrity and accuracy of journal entries recorded in the general ledger. Applies to all manual journal entries (those not automatically from sub-systems) each period.	– **Documentation:** Every manual journal entry (JE) must have a documented explanation and relevant supporting evidence (invoices, calculations, etc.) attached or referenced. – **Approval:** JEs are prepared by one person and reviewed/approved by another (segregation of duties). Higher-value or high-risk entries may require higher management approval. – **Timeliness:** JEs should be posted and approved within the timeframe of the monthly close schedule. Any JEs for a period must be completed before that period is finalized. – **Accuracy:** The preparer and reviewer ensure the entry is correctly coded (proper account, department, etc.) and balanced. They verify that the entry aligns with GAAP and does not duplicate or omit transactions. – **Retention:** All JEs and their backup documentation are retained in the Journal Entry system for audit trail purposes, as per record retention policy.
Month-End Close Control Policy	Execute an orderly and controlled financial close process each month and quarter. Ensures completeness of financial results and identification of issues before reporting.	– **Close Schedule:** Finance publishes a fiscal close calendar with key deadlines for sub-ledger closings, journal entries, reconciliations, and management reviews. All departments must adhere to this timeline. – **Prior Planning:** Before close, there are planning meetings to ensure all planned transactions (such as accruals, adjustments) are identified and necessary resources are in place to meet deadlines. – **Processing Transactions:** During the close window, all routine transactions (accounts payable, payroll, sales entries, inventory adjustments) are processed to capture the period's activity fully. – **Review and Issue Resolution:** Finance managers review preliminary financial results for anomalies or errors. Any significant accounting issues identified (e.g., unexpected variances, potential misstatements) are analyzed and addressed with corrective entries if needed to remediate risk of misstatement. – **Management Sign-off:** Division or department heads sign off on their

		financial results (budgets vs actuals, etc.). The CFO or Controller performs a final overall review. – **Adjustments and Lockdown:** Once all entries are posted and reviewed, the period is closed in the system to prevent further changes. Late adjustments, if absolutely necessary, require CFO approval and are documented.

(These policies are part of Zava's internal finance manual. They align with the objective of delivering timely, accurate US GAAP financial results each period, similar to our holding company's approach . Adherence is mandatory for all finance personnel. Internal Audit periodically tests compliance with these policies, and non-compliance is addressed by leadership.)

By enforcing the above policies, Zava significantly **mitigates the risk of financial errors or fraud**. For instance, timely account reconciliations help catch any anomalies on the balance sheet (like improper balances or missing transactions) before they flow into published reports . Proper journal entry controls prevent unsupported or incorrect entries that could misstate results. A disciplined close process ensures that nothing falls through the cracks when books are finalized each month or quarter. Together, these controls contribute to the reliability of Zava's financial reporting and feed into the larger SOX compliance effort.

Data Governance and Privacy

In the digital age, data is a critical asset for any company, including retail businesses like Zava. Zava has established a **Data Governance Policy** to ensure that data is managed responsibly, securely, and in compliance with all relevant privacy and data protection laws. This policy recognizes that data (whether customer information, employee records, sales data, or operational metrics) must be handled with care to maintain trust and meet legal requirements.

Data as an Asset: Zava treats data as a vital organizational resource that supports business adaptability and informed decision-making . The Data Governance Policy provides definitions to clearly scope what is considered a data asset. For example, **structured data** (such as databases, spreadsheets, system logs) and **master data** (core reference information like product catalog, customer lists, etc.) are within the governance scope, while unstructured content (documents, images) may be governed by other content management policies . By defining terms like data asset, structured data, unstructured data, and metadata, Zava ensures everyone speaks the same language regarding data management.

Ownership and Stewardship: Every key dataset or system in Zava's environment has an assigned **data owner** (and possibly a data steward) responsible for its quality and compliance. Clear ownership means someone is accountable for access control, regular

quality checks, and lifecycle management of that data asset . For instance, the customer database might be owned by the Head of Customer Analytics, while sales transaction data is owned by the CFO's team. Data owners work in conjunction with IT and compliance teams to enforce governance standards.

Data Governance Principles: The policy outlines several core principles (mirroring those in the reference document) that guide how data is handled :

- **Discoverability:** All important data should be catalogued and easily discoverable by authorized personnel. Zava maintains a Data Inventory or Catalog where datasets are listed along with their owners, descriptions, and applicable controls. This prevents "unknown" data silos and helps in compliance (e.g., knowing where personal data resides for privacy law purposes).
- **Quality:** Data must be accurate, consistent, and reliable. Zava enforces validation rules, routine data cleaning, audits for discrepancies, and uses automated tools (like a Data Health Dashboard) to monitor data quality metrics . Poor data quality can lead to bad decisions or compliance failures, so this is treated seriously.
- **Access and Security:** Data access is governed by the principle of least privilege – only those with a need to use data get access, and even then at the minimal level necessary. Access rights to databases and reports are reviewed periodically to revoke any unnecessary permissions. Sensitive data (like personal identifiable information, payment details, or confidential business data) is protected with encryption, strong authentication, and network security measures. Any system holding customer personal data is designed to meet security standards and undergoes risk assessments.
- **Compliance:** All data must be handled in compliance with applicable **legal, regulatory, and contractual requirements**. This is a critical point: for instance, customer personal information will be managed in line with privacy laws such as the California Consumer Privacy Act (CCPA)/California Privacy Rights Act and other data protection regulations. Zava's policy mandates that for each dataset, one must consider what regulations apply (financial data for SOX, cardholder data for PCI DSS, personal data for privacy laws, etc.) and ensure the handling meets those requirements. If Zava engages in analytics or uses AI, it also considers ethical guidelines for data use.
- **Lifecycle Management:** Data is managed through its entire lifecycle from creation/collection, to usage and storage, and ultimately to archival or deletion. Zava defines retention schedules for various types of data (e.g., financial records kept for 7 years for audit/tax purposes, customer data retained only as long as needed for business or as required by law). When data is no longer needed, it is disposed of securely. The policy also covers data accuracy over time – for example, master data like product information is kept up-to-date to avoid inconsistencies.

Privacy and Personal Data Protection: As a retailer, Zava collects personal data from customers (names, contact info, purchase history, perhaps payment info in tokenized form, etc.) and from employees. Zava is committed to protecting this personal information. The company abides by privacy principles such as **notice and consent**, purpose limitation, data minimization, and individual rights. In practice:

- Zava has a **Privacy Policy** for customers that transparently discloses what data is collected and why, how it is used, and how it is stored. Customers are given appropriate notice (e.g., on the website or at point of sale) and choices (like email marketing opt-ins).
- Personal data is used only for legitimate business purposes for which it was collected (e.g., fulfilling orders, improving services, marketing with consent).
- Zava minimizes the personal data it stores – collecting only what is necessary (for instance, keeping payment info only via secure payment processors rather than storing full credit card numbers internally).
- For any sensitive personal data, additional safeguards are in place and access is highly restricted.
- If individuals (customers or employees) have rights under law (like the right to access or delete their data under CCPA or similar laws), Zava has processes to respond to those requests within required timeframes.
- Data breach response plans exist: if there is ever a security incident, Zava can quickly inform affected individuals and authorities as required by law.

Zava likely follows frameworks such as the **PCI DSS** (for payment data, covered in the next section) and may also align with industry standards like ISO 27001 for information security management, which complements data governance by providing structure to protect data confidentiality, integrity, and availability.

On the **procedural side**, Zava's Data Governance Policy requires regular compliance assessments:

1. **Inventory and Classification:** All data systems must be registered in a central inventory (as noted) and data classified (public, internal, confidential, highly confidential) to determine handling rules.
2. **Compliance Reviews:** The data governance team runs periodic reviews using tools (like the Data Health Dashboard mentioned) to check if data systems are meeting the standards for quality, documentation, security, etc. .
3. **Remediation:** If a gap is found (say a dataset without a clear owner, or a database with outdated access controls), the responsible team must implement corrective actions. The governance team assists and tracks completion of these actions.
4. **Support and Guidance:** The Data Governance office at Zava is available to help with any compliance issues or technical challenges in implementing these policies.

Overall, Zava's approach to data governance ensures that **data-driven decisions are trustworthy and legally compliant**, and it minimizes risks such as data breaches, privacy violations, or loss of data quality. This not only protects Zava from legal penalties but also strengthens the confidence of customers, partners, and regulators in how Zava handles information.

Payment Infrastructure and Security Compliance

Retail operations involve extensive handling of payments and financial transactions. Zava has a dedicated **Payment Infrastructure, Compliance, and Security Policy** to govern all aspects of how payments are accepted, processed, and secured. The policy covers the use of various payment instruments (credit/debit cards, electronic fund transfers, checks, cash, mobile wallets, etc.) and ensures compliance with financial industry regulations and security standards, notably the **Payment Card Industry Data Security Standard (PCI DSS)** for credit card transactions.

Scope and Purpose: The Payment Policy's purpose is to protect both the company and its customers by ensuring that payment processes are secure and compliant. It applies to any system or process where Zava collects customer payments – whether in-store point-of-sale systems, e-commerce payment gateways on its website, or any alternative payment methods it might accept.

PCI DSS Compliance: Because Zava processes credit and debit card payments, it must adhere to PCI DSS, a stringent set of security standards created by major credit card brands. Zava's policy mandates:

- All systems that **store, process, or transmit cardholder data** must be configured and maintained in accordance with PCI DSS requirements. This includes maintaining secure networks (firewalls, no default passwords), protecting cardholder data (encryption of data in transit and at rest, masking of PAN, etc.), regular vulnerability management (anti-virus, patching), strong access control measures (unique IDs, limited access to card data on need-to-know), continuous monitoring and testing of networks, and having an information security policy.
- **Annual PCI Audit:** Zava undergoes an independent audit each year (by a Qualified Security Assessor) to verify PCI DSS compliance, as required for a Level 1 merchant (typically processing large volumes of card transactions). The successful completion of this audit demonstrates that Zava's controls around payment security are in place and working. Any deficiencies found are remediated immediately and re-tested.
- **Segmentation of Cardholder Data Environment:** The policy requires that systems handling card data are isolated in a secure network zone (often called the CDE – Cardholder Data Environment). Only necessary systems can communicate with this zone, minimizing the risk of breach spreading. For example, the databases storing

card tokens or the payment processing servers are kept separate from the corporate IT network.

- **Secure Development:** Any software or application that touches payment information must go through security review and testing (including code review, penetration testing) to ensure it doesn't introduce vulnerabilities.
- **Incident Response:** There is a defined incident response plan specifically for payment data breaches. Employees know how to escalate any suspected issue (like a point-of-sale malware detection) and a team is in place to contain and investigate such incidents, with obligations to notify banks or customers as necessary.

Other Payment Regulations: Beyond PCI DSS, Zava complies with all applicable financial regulations related to payments. This can include **anti-money laundering (AML) rules** and the Bank Secrecy Act (e.g., certain cash transaction reporting if applicable), **NACHA rules** for electronic transfers, and any state regulations on gift cards or prepaid cards. While these may not all be directly cited in the policy, the compliance team ensures these aspects are covered in procedures (e.g., ID verification for large cash refunds to prevent fraud, etc.).

Vendor and Partner Compliance: Zava uses third-party payment processors and banks for handling transactions. The policy states that any such **vendors, acquirers, or partners who process or store Zava's customer payment data must be PCI DSS compliant** at a Level 1 standard as well. Zava requires proof of compliance (certifications or audit reports) from these third parties annually. Contracts with payment service providers include clauses that they follow industry security standards and notify Zava of any security incidents. This extends Zava's security umbrella outward to all parties in the payment chain.

Payment Data Retention: In alignment with the principle of data minimization, Zava does not keep sensitive payment data longer than necessary. The policy sets a maximum retention period (for example, our holding company's policy specifies 18 months + 1 day, and Zava adopts a similar or shorter period) for retaining cardholder data (likely card token, transaction logs without full PAN, etc.) unless required for business (like recurring billing) or disputes. After that, data is securely deleted. Any paper records with card data (if they exist, e.g., receipts) are securely stored and destroyed as per schedule.

Security Controls: Some specific security controls highlighted by the policy:

- **Encryption:** All credit card numbers are encrypted or tokenized. If Zava's e-commerce site accepts cards, it likely uses a payment gateway that tokenizes card numbers, so Zava's systems never see raw card data. In stores, card readers are EMV compliant and encrypt data at swipe/tap.
- **Access Restrictions:** Only a very limited set of operations and IT personnel have access to systems with card data, and such access is granted after background checks and training, and is monitored.

- **Network Monitoring:** Intrusion detection systems monitor the payment networks for suspicious activity. Regular scans and penetration tests are conducted (PCI requires quarterly vulnerability scans and annual penetration tests).
- **Physical Security:** If any servers or storage media with card data exist on-premises, they are kept in secure facilities with badge access, CCTV, etc.
- **Compliance Monitoring:** In addition to the annual PCI audit, Zava might run internal compliance checks, like monthly reviews of user accounts on payment systems, or change management reviews for any updates to those systems.

Cash and Other Payments: While electronic payments require heavy security, Zava also covers controls for other payment types. For cash handling, there are controls to reduce theft (e.g., dual custody when counting cash, daily reconciliations of register cash, armored transport for bank deposits). For checks or bank transfers, Zava uses positive pay and other fraud prevention tools in coordination with its banks.

Taken together, these measures drastically reduce the risk of **payment fraud, data breaches, or financial loss**. They also ensure Zava meets the expectations of credit card companies and instills confidence in customers that their payment information is safe when they shop with Zava. Maintaining PCI DSS compliance is not only a legal/contractual requirement for accepting cards but also a hallmark of a mature security posture in the retail industry.

In summary, **information security** at Zava extends beyond payments: the IT department has a wider cybersecurity program to protect all systems (with policies on password management, phishing training, incident response, etc.). But the Payment Infrastructure Security Policy zeroes in on the highest sensitivity area – customer payment data – and satisfies the strict criteria of that domain.

Risk Management and Internal Audit

Managing risk is an integral part of Zava's governance framework, cutting across all areas discussed (strategy, operations, finance, compliance, etc.). Zava has an **Enterprise Risk Management (ERM)** process to systematically identify, assess, and mitigate risks that could affect the company's ability to achieve its objectives. This includes financial risks, operational risks (like supply chain disruptions or IT downtime), compliance risks (legal or regulatory penalties), reputational risks (brand damage from a scandal or breach), and strategic risks (e.g., failing to adapt to market changes).

Board and Management Roles in Risk Management: The Board of Directors, as noted, has ultimate oversight of risk management. At least annually, the Board or its Risk Committee reviews the company's risk profile – major risks and the plans in place to manage them. Management, on the other hand, is responsible for executing risk management activities day-to-day. Zava's executive team embeds risk thinking into decision making (e.g., before launching a new initiative, they consider legal and safety risks; finance regularly reviews

credit risk from partners, etc.). A Chief Risk Officer may not exist as a separate title, but the CFO or another executive often coordinates the ERM program.

Risk Assessment Process: Zava conducts enterprise risk assessments periodically. This might involve workshops or interviews with department heads to surface what they see as top risks in their areas, analysis of industry trends and external factors, and evaluating any incidents from the past. Risks are typically prioritized by likelihood and impact. For example, a data breach might be high impact, medium likelihood; a compliance violation for a new regulation might be medium impact, high likelihood if not well prepared. The result is a risk heat map that is presented to leadership.

Risk Mitigation: For each significant risk, Zava decides on a mitigation strategy: avoid, reduce, transfer, or accept. Most often, the company will implement controls or initiatives to **reduce** the risk to an acceptable level. Many of the policies described earlier are in fact risk mitigations (e.g., the Code of Conduct and training reduce the risk of ethical breaches; internal controls reduce financial misstatement risk; PCI compliance reduces security breach risk). The ERM process ensures there is an owner for each major risk and actions taken. Some risks are transferred via insurance (Zava likely carries cyber liability insurance, general liability, product liability insurance, etc. to cushion financial impact if adverse events occur).

Continuous Monitoring: Risk management is not a one-time activity. Key risk indicators (KRIs) are identified for top risks and monitored. For instance, for compliance risk, a KRI might be "number of regulatory notices or fines per quarter"; for cybersecurity risk, metrics like "number of high-severity vulnerabilities unpatched". If these indicators exceed thresholds, it triggers management action and possibly Board notification.

Internal Audit Function: Zava's Internal Audit (IA) department is an independent group reporting functionally to the Audit Committee and administratively to the CFO. Internal Audit provides assurance that controls are adequate and effective. It develops an **audit plan** each year focusing on high-risk areas. This often includes:

- Testing of financial controls (beyond what external auditors do for SOX, IA might look at controls in operations or compliance).
- Compliance audits (e.g., checking if data privacy procedures are being followed, or if store operations comply with safety regulations).
- Operational audits (e.g., assessing efficiency and controls in supply chain management or inventory).
- Special investigations if any signs of fraud or misuse appear.

After each audit, IA reports findings and recommendations. Management must respond with remediation plans for any control weaknesses or process improvements identified. Internal Audit tracks these to completion and reports unresolved issues to the Audit Committee to ensure accountability.

Incident and Crisis Management: Part of risk governance is having plans for when things go wrong despite prevention. Zava has crisis management and business continuity plans for various scenarios: data breach (as mentioned), natural disasters affecting operations, product recall procedures if a product is found defective, etc. These plans designate teams and actions to take immediately to mitigate damage and keep the business running. Regular drills or simulations might be conducted for preparedness.

Insurance and Contingency: As noted, insurance is used to transfer some risk. But Zava also sets aside contingency budgets or reserves for certain risks (for example, a legal reserve if they anticipate litigation exposure). The CFO monitors financial risk exposure such as foreign exchange (if any international business), interest rates (on any debt financing), and credit risk of large wholesale customers or vendors.

Integration with Strategy: Finally, risk management is tied into strategic planning. When the Board discusses major strategic moves (like expanding to a new market or launching a new product line), a formal risk review is part of the approval process. This ensures decisions are made with eyes open to potential downsides and with mitigation strategies ready.

Through proactive risk management and a vigilant internal audit function, Zava strives to **prevent surprises** that could threaten its stability. This discipline helps maintain smooth operations and protect shareholder value. It also reassures investors, customers, and regulators that Zava is not recklessly exposing itself to avoidable risks.

Enforcement, Review, and Continuous Improvement

Zava's governance policies and procedures are not static; they are living processes that undergo regular review and improvement to adapt to new challenges, business changes, or regulatory developments. Key points regarding the maintenance of this governance framework:

- **Policy Enforcement:** Each policy described (whether it's a financial policy, data policy, etc.) includes an **enforcement mechanism**. Typically, managers at various levels are responsible for ensuring their teams comply. For instance, the Controller enforces finance policies in their organization, the CISO (Chief Information Security Officer) enforces security policies in IT, and HR helps enforce the Code of Conduct. Violations of policies can lead to disciplinary action. For example, if an employee were to willfully ignore internal controls or commit an unethical act, they could face immediate termination . Consistent enforcement is critical — exceptions are not made for "high performers" or leaders; rules apply to everyone.
- **Regular Review and Updates:** Zava commits to reviewing its governance documents at least annually. The policies often have a "Document History" (as seen in our holding company's policies) noting revision dates. Changes in laws (like a new data privacy law or updates to GAAP) will prompt an update to relevant policies. Similarly, if an internal audit or incident reveals a gap, the policy will be revised. For example,

if a new form of electronic payment emerges and gains popularity, Zava's payment policy will be updated to address it. Each policy has an owner (person or department) responsible for keeping it current.

- **Board Oversight of Policy Changes:** Material changes to core governance policies are approved by the Board or relevant Board committee. For instance, if Zava wanted to relax a control or take a significantly different approach, senior management would need to justify this to the Board. This prevents erosion of controls over time.
- **Continuous Improvement:** The company fosters a culture of continuous improvement in governance. Employee feedback is welcomed when policies are overly burdensome or unclear, so that they can be refined without sacrificing control objectives. Technological solutions are also leveraged – e.g., using automation to perform controls more efficiently (like automatically flagging unreconciled items), or adopting governance, risk, and compliance (GRC) software to track compliance tasks.
- **External Benchmarks:** Zava may benchmark its governance practices against industry peers or frameworks (COSO for internal control, ISO standards for compliance, etc.) to ensure it meets or exceeds common practices. Also, lessons learned from any public failures at other companies (for example, if a competitor suffered a big compliance fine, Zava would proactively double-check its own compliance in that area).

By enforcing its policies strictly yet fairly, and by keeping its governance framework up-to-date, Zava ensures that this is not just a document on a shelf, but a **day-to-day operational reality**. The company's leadership understands that strong governance is a journey, not a destination – it requires ongoing attention and adaptation. This mindset is what allows Zava to remain resilient and reputable in a dynamic business and regulatory environment.

Conclusion:

Zava's legal governance document brings together all critical components of a sound governance and compliance system for a U.S.-based retail corporation. From the Boardroom to the stock room, ethical conduct and compliance are emphasized and reinforced with concrete policies. The corporate governance structure provides clear oversight and accountability. Robust financial controls and reporting practices ensure transparency and accuracy in the company's financial communications to stakeholders . Data governance and security safeguards protect the lifeblood of the modern enterprise – information – thereby maintaining customer trust and meeting legal mandates . Compliance with laws and regulations is integrated into the fabric of operations, reducing legal risk and enhancing Zava's reputation as a principled market player .

This governance framework not only serves to keep Zava on the right side of the law, but it also **creates business value**: it improves decision-making through better data, protects the company from financial malpractices, and fosters an ethical culture that can attract

investors, employees, and customers. It is a living framework – regularly reviewed and improved – ensuring that Zava can adapt to new challenges while holding true to its core values of integrity, responsibility, and excellence in execution.

By adhering to this comprehensive governance program, Zava is well-positioned to operate effectively, comply with its obligations, and achieve long-term success in the retail industry. The above document provides a model that can inform the development of AI agents focused on legal and compliance tasks, as it encapsulates the many rules and policies those agents would need to consider.