Compliance Requirements for Code Review

The following criteria must be met for code to be considered compliant under modern security and privacy frameworks:

1. GDPR Compliance
   - No plaintext storage of personal or sensitive user data.
   - Consent and data minimization should be considered.
   - Sensitive fields like passwords or credit card data must be encrypted.

2. ISO/IEC 27001 & SOC 2 Security Requirements
   - All file operations should include secure handling (use of context managers).
   - No use of unsafe functions like eval() or exec().
   - Logging should be implemented for key actions and access to sensitive operations.

3. Software Development Quality Standards
   - Each function must have a docstring explaining its purpose.
   - Constants (like discount rates) should not be hardcoded; use named constants.
   - Configuration files should not be written to from within code without access controls.

4. Industry-Specific Requirements (e.g. FinTech, HealthTech)
   - Sensitive information such as credit card data must never be logged.
   - Any processing of financial data should follow PCI-DSS principles.
   - Access and identity operations should have audit trails.

All code submitted should be reviewed against this checklist.