POLÍTICA ORGANIZACIONAL

Assunto: Gestão de Riscos, Controles Internos e Compliance	**Identificação:** PO-GC-03 **Versão:** 05
Diretoria Responsável: Controles Internos, Riscos e Compliance	**Publicado em:** 05/05/2026
Normas vinculadas:	**Revisão até:** 05/05/2029

1. Objetivo

Esta política tem por objetivo estabelecer os princípios, as diretrizes e responsabilidades a serem observadas no processo de gestão de **Riscos** corporativos, **Controles** Internos e **Compliance**, bem como disseminar a **Cultura de Gestão de Riscos** e o **Programa de integridade** por todos os níveis da TOTVS.

2. Abrangência

Esta Política aplica-se a todas as áreas da TOTVS, aos seus respectivos empregados e administradores, bem como às suas subsidiárias integrais, sendo que as regras aqui estabelecidas devem ser reproduzidas nas políticas das controladas diretas e indiretas, no Brasil e nos demais países, sempre respeitando seus documentos constitutivos e a legislação local aplicável.

Deve-se garantir, ainda, que **Terceiros**, subcontratados, representantes, consultores, fornecedores e prestadores de serviço de qualquer natureza, quando do seu relacionamento com ou representando a TOTVS, também pautem suas ações no disposto nesta Política.

3. Referências

- ABNT (Associação Brasileira de Normas Técnicas) NBR ISO 31000:2018: Gestão de Riscos – Princípios e Diretrizes.
- CODEC - Código de Ética e Conduta da TOTVS.
- Código Brasileiro de Governança Corporativa das Companhias Abertas - Instituto Brasileiro de Governança Corporativa – "IBGC".
- COSO ERM - Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management Framework.
- Decreto 11.129/22 – Decreto que regulamenta a Lei Anticorrupção.
- Estatuto Social da TOTVS.
- IBGC: Cadernos de Governança Corporativa, Gerenciamento de Riscos Corporativos e Compliance à luz da Governança Corporativa.
- Lei 12.846/13 – Lei Anticorrupção Brasileira.
- Portaria CGU 909 – Avaliação de programas de integridade de pessoas jurídicas.

4. Definições

Alta Administração: membros do Conselho de Administração e Diretoria Estatutária.
Apetite ao Risco: se refere ao nível de risco que a Companhia está disposta a incorrer para atingir seus objetivos estratégicos. O Apetite ao Risco na Companhia é definido e mensurado de forma qualitativa.
Canal de Ética e Conduta: canal para que toda pessoa que se relaciona direta ou indiretamente com a TOTVS (incluindo colaboradores, acionistas, clientes, fornecedores, franqueados e parceiros e seus colaboradores e quaisquer terceiros) possam comunicar de forma confidencial, situações que

possam caracterizar violação do Código de Ética e Conduta da TOTVS ou qualquer outro ato que infrinja ou possa infringir a Legislação e/ou Regulamentação vigentes.

Colaborador ou Colaboradores: para fins desta Política, significam todos os empregados que trabalham na TOTVS.

Compliance: deriva do verbo inglês "*to comply*", que significa conformidade, que é o dever de cumprir e fazer cumprir leis, decretos, regulamentos e instruções aplicáveis às atividades da TOTVS.

***Control Self-Assessment (CSA)*:** a autoavaliação de controles é uma metodologia/técnica utilizada para avaliar o desenho e a eficácia operacional dos controles internos. Ela envolve um questionário respondido pelos gestores das áreas de negócio com a finalidade de auto avaliar tanto os controles internos quanto os riscos envolvidos nos processos sob sua responsabilidade.

Controles Internos: é o conjunto de atividades e controles manuais e sistêmicos que compõem uma barreira de proteção para que as atividades operacionais e tomadas de decisões sejam realizadas em um ambiente seguro e para que os riscos sejam rapidamente identificados e tratados.

Cronograma anual de Compliance: planejamento estabelecido visando determinar a priorização das ações previstas no Programa de Integridade.

Cultura de Gestão Riscos: conjunto de padrões éticos, valores, atitudes e comportamentos aceitos e praticados, e à disseminação da gestão de riscos como parte do processo de tomada de decisão em todos os níveis.

Dicionário de Riscos Prioritários: referência padronizada para identificar, categorizar e organizar os eventos de risco que podem afetar os objetivos estratégicos da companhia.

Diretoria Estatutária: Diretor-Presidente e Vice-Presidentes da TOTVS.

Dono do Risco: responsável pela execução dos controles internos para garantir que o risco seja gerenciado adequadamente e pela definição e implementação dos planos de ação necessários para a remediação e/ou minimização dos riscos, bem como pelo monitoramento contínuo e identificação de novos riscos.

Entes Públicos: qualquer órgão ou entidade vinculados direta ou indiretamente a algum dos Poderes da Administração Pública Nacional ou Estrangeira, tais como, mas não se limitando, à União, o Distrito Federal, os estados, os municípios e as representações diplomáticas de país estrangeiro. Também se incluem nesse conceito as pessoas jurídicas controladas por esses órgãos ou entidades, ainda que constituídas com personalidade jurídica de direito privado, como, por exemplo, as autarquias, as estatais, as fundações, as associações e os organismos internacionais.

Estrutura Normativa Interna: composta pelos documentos normativos que estabelecem as políticas, normas, diretrizes, regras, procedimentos, modelos e métodos com a finalidade de direcionar a interação dos Colaboradores em suas atividades, em consonância com os valores, cultura, estratégia da TOTVS e de acordo com a regulamentação vigente.

Exposição ao Risco: quantificação da possibilidade da TOTVS ser afetada por determinado Risco.

Fator de Risco: fator interno ou externo que pode originar os Riscos.

Impacto: refere-se ao resultado ou consequência caso ocorra a materialização de um evento de risco. O impacto do risco é analisado em diferentes esferas, conforme a régua definida.

Indicadores Chave de Risco (KRIs): indicadores utilizados para medir e monitorar dados associados aos riscos, podendo ser de caráter preditivo/preventivo, quando possuem métricas que apontam uma tendência à sua materialização, ou detectivo, no caso de indicadores que informam riscos já materializados.

Matriz de Riscos: consiste em uma representação gráfica do inventário dos riscos mapeados, classificados em quadrantes de acordo com suas probabilidades de materialização e seus impactos.

Mudanças Climáticas: referem-se às alterações de longo prazo nos padrões de temperatura e clima, podendo ter origem em causas naturais ou como consequência de atividades humanas.

Oportunidade: evento que possa impactar positivamente a realização dos objetivos da TOTVS, contribuindo para a criação e preservação de valor.

Plano de Ação: ação ou conjunto de ações visando a mitigação ou redução do nível de exposição de um risco identificado, podendo ser um projeto, ação específica ou controle do processo (ação contínua).

Probabilidade: nível qualitativo ou quantitativo que define a possibilidade de materialização de um evento de risco.
Programa de Integridade: conjunto de mecanismos internos de integridade, com o objetivo de prevenir, detectar e combater fraudes, corrupção e demais atos ilícitos praticados no âmbito privado ou público, conforme regulamentação vigente, no Brasil e/ou no exterior, nos locais em que a TOTVS possui atuação.
Risco: Evento que possa afetar negativamente os resultados da TOTVS e sua capacidade de atingir seus objetivos estratégicos e de negócios.
Terceiro(s): qualquer pessoa física (que não seja colaborador) ou jurídica que tenha qualquer relação com a TOTVS, incluindo franquias.
Tolerância a Riscos: nível máximo de exposição à riscos que a entidade está disposta a incorrer no aproveitamento de Oportunidades e na busca e realização de sua estratégia.
TOTVS ou Companhia: significa a TOTVS S.A, suas subsidiárias e controladas diretas e indiretas, de forma individual ou coletiva no Brasil ou no exterior, com exceção da empresa TOTVS Techfin.

5. Diretrizes

- A TOTVS é comprometida com uma conduta ética em seu relacionamento com **Colaboradores**, clientes, parceiros, fornecedores, investidores, **Entes Públicos** e demais partes interessadas e com o cumprimento das leis e regulamentação aplicável, incluindo, mas não se limitando, à lei anticorrupção e as Políticas, Normas e Procedimentos internos da Companhia;
- O processo de gerenciamento de **Riscos** e controles internos deve fornecer subsídios para tomada de decisões visando a mitigação ou redução do nível de **Exposição aos Riscos** e a adequada priorização de ações;
- As informações utilizadas para o gerenciamento dos **Riscos** e controles internos devem ser íntegras e corretas, representando a situação atual das operações da TOTVS;
- Os **Riscos** da Companhia devem ser comunicados a todos os envolvidos em seu gerenciamento e monitoramento, bem como reportados tempestivamente.

A área de Controles Internos, Riscos e Compliance reporta-se diretamente ao Diretor-presidente da TOTVS, goza de independência e autonomia para executar as atividades relativas ao **Programa de Integridade**, dispondo, inclusive, de acesso irrestrito às informações necessárias para suas atribuições, sendo as referidas premissas ratificadas pelo apoio da Alta Administração da TOTVS.

5.1. Gestão de Riscos

5.1.1. Categoria de Riscos

A Companhia categoriza seus **Riscos** conforme descritos abaixo, considerando fatores externos e internos.

Risco Estratégico: eventos de **Riscos** associados às decisões que afetam a estratégia de negócios ou os objetivos estratégicos da TOTVS, considerando o ambiente interno e externo.
Risco Operacional: referem-se às possíveis perdas resultantes de interrupções, falhas, deficiências ou inadequação de processos internos, pessoas, ambiente organizacional, tecnológico ou provocadas por eventos externos, incluindo o risco físico às instalações.
Risco Financeiro: está associado à exposição a potenciais perdas financeiras da TOTVS.
Risco Regulatório/de Compliance: Riscos de sanções legais ou regulatórias, de perda financeira ou de reputação que a TOTVS pode sofrer como resultado de falhas no cumprimento da aplicação de leis, acordos, regulamentos, Código de Ética e Conduta, dentre outros.
Riscos de Tecnologia da Informação: Riscos relacionados ao ambiente de tecnologia da informação (incluindo, mas não se limitando à infraestrutura, gestão de acessos, segurança da

informação, uso de inteligência artificial) que podem impactar os negócios da TOTVS, como a ocorrência de ciberataques, vazamentos, indisponibilidade do ambiente de TI e obsolescência tecnológica.

5.1.2. Metodologia e Processo de Gestão de Riscos

A metodologia de gestão de **Riscos** aplicada na TOTVS é suportada por um modelo híbrido que contempla os componentes descritos no COSO ERM (*Enterprise Risk Management*) e na ISO 31000. Esta abordagem estabelece um framework para a gestão integrada e contínua de **Riscos** corporativos, estruturado em 6 (seis) etapas essenciais, além de aspectos de cultura e governança, conforme detalhado a seguir:

5.1.2.1. Estabelecimento do Contexto

Etapa inicial do processo compreende a captura e entendimento dos objetivos estratégicos, considerando fatores do ambiente interno e externo que possam impactar o atingimento desses objetivos em um horizonte de curto (1 ano), médio (2 a 3 anos) e longo prazo (4 a 5 anos), abrangendo tendências setoriais, mudanças tecnológicas, cenário macroeconômico, ambiente regulatório, aspectos de sustentabilidade e mudanças climáticas, bem como quaisquer outros fatores identificados na análise do cenário.

5.1.2.2. Identificação de Riscos

O processo de identificação de **Riscos** consiste na utilização de ferramentas específicas, como mapeamento de processos, entrevistas com os gestores responsáveis de cada área/segmento de negócio e com a Alta Administração, bem como o histórico de materialização de eventos de **Risco**. Este processo deve permitir a captura de riscos, com o intuito de estabelecer as matrizes de riscos e mantê-la constantemente atualizada, com base nos eventos que possam impactar os objetivos estratégicos de negócio da TOTVS.

Esta etapa deve assegurar, ainda, a correlação direta entre os **Riscos** identificados e os temas materiais da TOTVS, considerando aspectos financeiros e de sustentabilidade, utilizando o **Dicionário de Riscos Prioritários** como referência padronizada para a categorização.

5.1.2.3. Análise e Avaliação de Riscos

Os **Riscos** e respectivos **Fatores de Risco** associados são avaliados de acordo com a sua **Probabilidade** e **Impacto,** considerando as seguintes esferas:

- **Financeiro:** mensura a perda financeira direta, considerando os **Impactos** nos resultados operacionais da companhia;
- **Reputacional:** avalia o grau de exposição negativa da imagem da TOTVS perante o seu ecossistema (clientes, parceiros, investidores e **Colaboradores**) e a repercussão em mídias digitais ou veículos de comunicação;
- **Legal/Compliance:** analisa o **Impacto** decorrente de sanções legais ou regulatórias, processos judiciais ou administrativos, o descumprimento de licenças ou legislações vigentes, do Código de Ética e Conduta, dentre outros;
- **Operacional:** mede o nível de interrupção dos processos internos ou da prestação de serviços aos clientes, observando o tempo de recuperação da operação normal, incluindo eventos físicos que possam impactar a continuidade operacional; e

- **Segurança da Informação:** avalia danos à integridade, disponibilidade e confiabilidade de dados da própria TOTVS e de seus clientes, oriundos de incidentes cibernéticos ou vazamentos de informações.

Para classificação consolidada da **Probabilidade** e do **Impacto** do **Risco**, deve prevalecer o maior nível de criticidade identificado em cada um dos **Fatores de Risco** analisados. A atribuição da classificação final do risco ocorre por meio do cruzamento dos eixos de **Probabilidade** e **Impacto**, resultando em 4 níveis: (i) Baixo; (ii) Médio; (iii) Alto; e (iv) Crítico. Adicionalmente, a análise pode contemplar a visão de interconectividade entre os **Riscos** da matriz como um fator qualitativo para compreensão de possíveis **Impactos** em cadeia.

5.1.2.4. Tratamento dos Riscos

A definição de resposta ao risco envolve a elaboração, formalização e implementação de um ou mais **Planos de Ação** para mitigação dos eventos de **Riscos** pelas respectivas áreas responsáveis. O tratamento deve buscar a redução da **Probabilidade** e/ou do **Impacto** dos **Riscos** identificados, garantindo que as respostas sejam eficazes e que os recursos sejam utilizados de forma otimizada e alinhada aos objetivos estratégicos da TOTVS.

O processo de tratamento é subsidiado pelo eventual reforço nos **Controles Internos** e no estabelecimento de **Indicadores Chave de Risco (KRIs)** atrelados a **Riscos** ou **Fatores de Riscos** específicos, podendo um indicador monitorar mais de um evento simultaneamente. Nos casos em que o indicador não permita a definição de metas quantitativas, a avaliação baseia-se na análise qualitativa da tendência e no comportamento histórico do indicador.

Os riscos classificados como Altos e Críticos devem ser objeto de **Planos de Ação** para redução da classificação, devendo tais ações serem iniciadas no prazo máximo de 60 dias a partir da formalização do respectivo plano. Planos estruturantes para mitigação de **Riscos** Altos e Críticos, que dependam de recursos não disponíveis, projetos de TI de alta complexidade ou mudança organizacional, poderão ter prazos estendidos, mediante recomendação do Vice-Presidente da área responsável e aprovação do Comitê de Auditoria Estatutário. Neste caso, no prazo de 60 dias, devem ser adotados controles compensatórios temporários até a conclusão dos **Planos de Ação** definitivos.

O aceite de **Riscos** pela TOTVS ocorre quando a companhia decide manter o nível de exposição atual, sem a implementação de novas ações de mitigação. Essa decisão deve obedecer às alçadas de aprovação estabelecidas abaixo:

Classificação do Risco	Alçada para assunção de riscos - TOTVS		
	Recomendação	Aprovação do Aceite	Reporte/Informação
Crítico	Diretor-Presidente e Comitê de Auditoria Estatutário	Conselho de Administração	-
Alto			

Médio	Vice-Presidente Responsável pelo risco	Diretor-Presidente	Comitê de Auditoria Estatutário
Baixo	Diretor ou Head responsável pelo risco	Vice-Presidente Responsável pelo risco	Diretor-Presidente
Muito Baixo			

5.1.2.5. Monitoramento e Reporte

O monitoramento adequado dos **Riscos** visa garantir a eficácia das ações adotadas e a comunicação tempestiva às partes interessadas, sendo composto pelos seguintes pilares:

- Acompanhamento constante do ambiente de **Controles Internos** da Companhia, por meio do mapeamento de **Riscos** e controles;
- Execução e monitoramento das ações de resposta aos **Riscos** (**Planos de Ação** e/ou controles), cuja efetividade é acompanhada pelas áreas responsáveis com o suporte da área de Controles Internos, Riscos e Compliance, responsável por reportar o status consolidado ao Comitê de Auditoria Estatutário da TOTVS; e
- Estruturação e monitoramento de **Indicadores Chave de Risco (KRIs)**, definidos pelas áreas responsáveis pelos **Riscos** em conjunto com a área de Controles Internos, Riscos e Compliance. Os KRIs subsidiam a avaliação dos níveis de **Probabilidade** e **Impacto** dos riscos e a identificação da necessidade de **Planos de Ação** adicionais, visando manter os riscos em níveis considerados aceitáveis pela TOTVS. Os **KRIs** devem ser utilizados pelos **Donos dos Riscos** para auxiliar na tomada de decisão e no fortalecimento da **Cultura de Gestão de Riscos**.

A prorrogação de prazos para conclusão de **Planos de Ação** deve ser precedida de justificativa formal pela área responsável e reportada ao Comitê de Auditoria Estatutário. Em se tratando de **Riscos** classificados como Altos e Críticos, o Comitê de Auditoria Estatutário deve comunicar ao Conselho de Administração da TOTVS os motivos e a nova previsão de conclusão dos referidos planos.

5.1.3. Ciclo de Revisão e Avaliação da Matriz de Riscos

A revisão da **Matriz de Riscos** deve ser realizada anualmente pela área de Controles Internos, Riscos e Compliance, observando os critérios de análise presentes nesta política, avaliada pelos Vice-Presidentes e Diretor-Presidente, e submetida à recomendação do Comitê de Auditoria Estatutário e à aprovação do Conselho de Administração.

Os **Riscos** contidos na nova **Matriz** devem ser objeto de **Planos de Ação** apresentados ao Comitê de Auditoria Estatutário e trimestralmente acompanhados quanto ao status de conclusão e análise da movimentação dos **Riscos** na **Matriz**. Cabe à área de Controles Internos, Riscos e Compliance verificar a implementação de tais **Planos de Ação**.

A área de Controles Internos, Riscos e Compliance deve também reportar periodicamente ao Comitê de Auditoria Estatutário e ao Conselho de Administração a evolução dos **Planos de Ação**, os **Indicadores Chave de Risco (KRIs)** apurados e o nível de **Exposição aos Riscos**. As apresentações e reportes devem obrigatoriamente constar na pauta anual do Comitê de Auditoria Estatutário e do Conselho de Administração, conforme o cronograma definido para cada exercício.

Este documento é propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é propriedade da TOTVS. Todos os direitos reservados. ©

5.2. Controles Internos

A estrutura de controle interno deve ser avaliada periodicamente, a fim de verificar a eficiência dos **Controles Internos** existentes e potenciais impactos decorrentes de mudanças no ambiente interno e/ou externo, considerando: (i) os objetivos estratégicos da Companhia; (ii) composição e natureza das contas contábeis; (iii) possibilidade de perdas decorrentes de erros e fraudes; e (iv) complexidade nas transações das contas contábeis.

5.2.1. Etapas da Gestão de Controles Internos

A área de Controles Internos, Riscos e Compliance deve mapear os processos, controles e realizar os testes de desenho dos controles (*"walkthroughs"*) e conduzir os testes de efetividade ("Testes de Controles"), com a finalidade de confirmar o entendimento dos processos mapeados, bem como se os controles estão implementados e funcionando de forma adequada.

Os controles inexistentes ou considerados insatisfatórios para mitigação dos **Riscos** identificados são reportados para as áreas responsáveis para elaboração de **Planos de Ação** visando a redução da **Exposição aos Riscos** e a melhora do ambiente de controles.

Concluídas estas etapas, os responsáveis pelos processos devem realizar anualmente o ***Control Self-Assessment*** (Autoavaliação de **Controles Internos**) no sistema utilizado pela TOTVS e, quando for o caso, apontar novos riscos identificados em seus processos ou atividades.

Todo o processo de mapeamento, revisão dos controles e seus respectivos resultados são reportados ao Comitê de Auditoria Estatutário da TOTVS.

5.3. Compliance

5.3.1. Programa de Integridade

O **Programa de Integridade** visa a assegurar que a legislação e regulamentação aplicáveis e as diretrizes e regras de conduta da TOTVS sejam conhecidas e cumpridas por todos os **Colaboradores**, bem como zelar para que os **Terceiros** com os quais a Companhia se relaciona compartilhem dos princípios éticos adotados pela TOTVS.

Anualmente, a área de Controles Internos, Riscos e Compliance reavalia as ações de cada um dos pilares do **Programa de Integridade** com o objetivo de identificar melhorias em seus processos. A referida avaliação ocorre mediante o monitoramento dos resultados e indicadores do Programa reportados aos órgãos de governança durante o ciclo anterior.

O **Programa de Integridade** da TOTVS está estruturado em 5 (cinco) pilares, conforme descrito a seguir:

5.3.1.1. Cultura de Integridade

Este pilar tem por objetivo fortalecer e disseminar uma cultura que esteja em conformidade com os padrões de ética e de integridade da TOTVS, por meio do engajamento e apoio constante da Alta Administração e das principais lideranças da TOTVS.

5.3.1.2. Avaliação de Riscos

Este pilar visa identificar e avaliar os principais **Riscos** do ponto de vista anticorrupção/**Compliance** aos quais a TOTVS está exposta, assim como mensurar seus **Impactos** e recomendar medidas

mitigatórias, considerando o cumprimento da legislação anticorrupção aplicável e as diretrizes de conduta estabelecidas no Código de Ética e Conduta e nas demais Normas do **Programa de Integridade**.

Os riscos de **Compliance** são reavaliados anualmente pela área de Controles Internos, Riscos e Compliance, visando monitorar os riscos relativos ao ciclo anterior, bem como identificar e tratar novos riscos eventualmente identificados.

5.3.1.3. Código de Ética e Conduta, Políticas e Procedimentos

Este pilar tem por objetivo estabelecer e formalizar as diretrizes, regras e procedimentos internos que devem ser seguidos pelos **Colaboradores** e **Terceiros** no âmbito do **Programa de Integridade**, formando a base de referência para que os mecanismos e controles de integridade sejam implementados e/ou otimizados.

5.3.1.4. Comunicação e Treinamento

O pilar de Comunicação e Treinamento visa a conscientizar e facilitar o desenvolvimento de uma **Cultura de Gestão de Riscos** e a compreensão dos **Colaboradores** quanto às diretrizes, regras e responsabilidades a serem cumpridas no âmbito do **Programa de Integridade** da TOTVS.

A área de Controles Internos, Riscos e Compliance deve elaborar e executar o Plano Anual de Comunicação e Treinamento considerando: (i) a relevância dos temas frente às diretrizes do Código de Ética e Conduta e demais Documentos Normativos; (ii) público-alvo; (iii) periodicidade e os canais de comunicação disponíveis; e (iv) a necessidade de reforço de temas identificados no histórico de ocorrência de eventos ou dúvidas relacionadas ao tema, se aplicável.

O Plano Anual de Comunicação e Treinamento deverá ser submetido à apreciação e validação do Comitê de Auditoria Estatutário e do Conselho de Administração, órgãos responsáveis pela supervisão da execução do plano por meio dos reportes da área de Controles Internos, Riscos e Compliance.

5.3.1.5. Detecção e Remediação

Este pilar visa identificar a ocorrência de condutas irregulares, ilegais, fraudes ou quaisquer outros descumprimentos à legislação e regulamentação aplicável e às Normas da TOTVS, bem como garantir a interrupção de tais condutas e a aplicação de medidas disciplinares e/ou corretivas, utilizando como principal instrumento um Canal independente ("**Canal de Ética e Conduta**") para recepção e tratamento de denúncias, disponível ao público interno e externo pelos telefones **0800 721 5966**, no Brasil, e **+55 11 3232 0766**, para demais localidades, ou através do site: **https://www.canalconfidencial.com.br/totvs/.**

A gestão do **Canal de Ética e Conduta** é realizada pela área de Controles Internos, Riscos e Compliance, a qual tem como atribuições principais: (i) recepcionar as denúncias para apuração das áreas responsáveis, de acordo com a natureza dos relatos; (ii) conduzir investigações nos relatos que tenham como objeto desvios comportamentais; e (iii) reportar as denúncias recebidas à Comissão de Ética e Conduta e aos demais órgãos de governança eventualmente aplicáveis.

Os casos de condutas irregulares são objeto de avaliação pela Comissão de Ética e Conduta da TOTVS, sendo que a área de Controles Internos, Riscos e Compliance possui independência funcional e pode ter acesso às reuniões da Comissão, números de investigações e tratativas de gestão de consequências.

6. Gestão de Consequências

Em caso de descumprimento desta Política ou os demais documentos que compõem a **Estrutura Normativa Interna** e a legislação e regulamentação aplicável, são adotadas medidas de gestão de consequências Trabalhistas, Cíveis, Criminais e Administrativas eventualmente aplicáveis aos responsáveis pelas ilicitudes, incluindo a possibilidade de demissão por justa causa e ruptura contratual por justo motivo no caso de franqueados e quaisquer **Terceiros** com os quais haja vínculo contratual.

7. Atribuições

Conselho de Administração

- Aprovar a Política de Gestão de Riscos, Controles Internos e Compliance;
- Aprovar os objetivos estratégicos e a metodologia de gestão de **Riscos** e **Controles Internos** e o **Programa de Integridade** da TOTVS;
- Determinar os níveis de apetite e de **Tolerância aos Riscos** propostos pela Diretoria e recomendados pelo Comitê de Auditoria Estatutário;
- Aprovar anualmente a **Matriz de Riscos** Prioritários tomando conhecimento das respectivas ações de gerenciamento adotadas e seus resultados, bem como os **Indicadores Chave de Risco (KRIs)** a serem monitorados;
- Aprovar a documentação de informações públicas sobre o modelo de gestão de **Riscos** e transparência de informações prestadas ao público interno e externo;
- Assegurar-se da existência de recursos adequados para o funcionamento eficaz do **Programa de Integridade** e garantir a autonomia da área de Controles Internos, Riscos e Compliance;
- Aprovar o plano anual de comunicação e treinamento elaborado pela área de Controles Internos, Riscos e Compliance;
- Acompanhar e deliberar sobre as recomendações do Comitê de Auditoria Estatutário a respeito dos resultados da Gestão de Riscos, Controles Internos e Compliance, além dos do **Programa de Integridade**; e
- Aprovar a assunção de **Riscos** Altos e Críticos.

Comitê de Auditoria Estatutário

- Avaliar esta Política e suas revisões e apresentar recomendação ao Conselho de Administração quanto à sua aprovação;
- Auxiliar a Diretoria na definição das diretrizes e metodologia de gestão de **Riscos** e **Controles Internos**, além das métricas de mensuração da **Tolerância** e **Apetite aos Riscos**, apresentando ao Conselho de Administração sua recomendação de aprovação;
- Avaliar os trabalhos de Gestão de Riscos e a construção da **Matriz de Riscos** Prioritários, apresentando ao Conselho de Administração suas recomendações;
- Avaliar e recomendar ao Conselho de Administração a fixação dos níveis de apetite e de **Tolerância aos Riscos**;

- Acompanhar e avaliar periodicamente os resultados dos testes de controles, os **Planos de Ação** mitigatórios e os **Indicadores Chave de Risco (KRIs)** apurados, reportando ao Conselho de Administração desvios e ocorrências consideradas relevantes;
- Discutir e aprovar o **Cronograma Anual de Compliance**;
- Avaliar e acompanhar os **Planos de Ação** da auditoria do **Programa de Integridade**;
- Reportar periodicamente, ao Conselho de Administração, casos críticos de desvios de conduta relativos à presente Política, bem como as eventuais medidas disciplinares adotadas; e
- Fazer recomendações ao Conselho de Administração quanto à assunção de **Riscos** Altos e Críticos.

Comissão de Ética e Conduta

- Acompanhar e avaliar os relatos das apurações e investigações das denúncias recebidas no Canal de Ética e Conduta da TOTVS;
- Deliberar sobre a procedência e gravidade das denúncias de violação ao Código de Ética e Conduta, à legislação e/ou demais normas internas da TOTVS e recomendar ao Diretor-Presidente a medida de gestão de consequência aplicável aos casos recebidos no Canal de Ética e Conduta.

Diretoria Estatutária e demais Diretorias

- Conduzir práticas de negócio que atendam à legislação e regulamentação aplicáveis e à **Estrutura Normativa Interna**;
- Apoiar na implementação e demonstrar comprometimento ao **Programa de Integridade**;
- Gerir os **Riscos** sob sua responsabilidade e auxiliar na criação de controles e ações mitigatórias; e
- Zelar para que as diretrizes de conduta da TOTVS sejam comunicadas e compreendidas pelos parceiros, franqueados, canais, clientes e demais **Terceiros**.

Controles Internos, Riscos e Compliance

- Propor alterações e submeter esta Política à aprovação;
- Estruturar, implementar, gerir e disseminar a metodologia de gestão de **Riscos** e o **Programa de Integridade**;
- Monitorar e reportar os **Planos de Ação** e os **Indicadores Chave de Risco (KRIs)** definidos para gerenciamento dos **Riscos**;
- Conscientizar os gestores e demais **Colaboradores** sobre a importância da gestão de **Riscos**, **Controles Internos** e do **Programa de Integridade**;
- Realizar o ciclo anual de **Controles Internos** nos termos desta Política;
- Atuar de forma independente e autônoma, de modo a garantir a imparcialidade em todas as suas atividades e reportar ao Diretor-Presidente e ao Comitê de Auditoria Estatutário caso algo interfira em sua independência;
- Compartilhar com a Auditoria Interna informações e/ou fatos sujeitos à investigação interna;

- Gerir as atividades do **Canal de Ética e Conduta** e reportar as denúncias à Comissão de Ética e demais órgãos de governança aplicáveis; e
- Reportar a **Matriz de Riscos** e os resultados do **Programa de Integridade** à Diretoria Estatutária, ao Comitê de Auditoria Estatutário e ao Conselho de Administração.

Auditoria Interna

- Avaliar a integridade das informações, a conformidade legal e a eficácia dos controles, assegurando a salvaguarda de ativos e o alinhamento dos processos aos objetivos estratégicos e de governança da TOTVS;
- Avaliar a eficácia dos processos de gestão de **Risco** da organização e dos planos de mitigação;
- Quando acionado, investigar denúncias recebidas do **Canal de Ética e Conduta** ou recebidas por qualquer outro meio;
- Compartilhar, caso solicitado, com a área de Controles Internos, Riscos e Compliance as não conformidades identificadas nos trabalhos de Auditoria; e
- Assegurar a independência funcional e a objetividade técnica, atuando sem interferências externas e reportando qualquer limitação à sua autonomia diretamente ao Comitê de Auditoria Estatutário.

Relações Humanas

- Fomentar e assegurar que os princípios do **Programa de Integridade** sejam disseminados junto à cultura organizacional da TOTVS.

Diretoria Jurídica

- Orientar a TOTVS em relação às normas emitidas pelos órgãos reguladores e às alterações legislativas, tanto federais, estaduais, como municipais;
- Relatar a ocorrência de ato que constitua ilícito administrativo, civil ou penal à Diretoria Estatutária e ao Conselho de Administração da TOTVS; e
- Apoiar a área de Controles Internos, Riscos e Compliance na interpretação das leis anticorrupção aplicáveis.

Donos dos Riscos/Áreas de Negócios e Operacionais

- Identificar continuamente e documentar os **Riscos** sob sua gestão;
- Realizar anualmente o **Control Self Assessment** dos processos sob sua responsabilidade;
- Comunicar à área de Controles Internos, Riscos e Compliance novos **Riscos** identificados e qualquer alteração em seu processo de negócio;
- Implementar, apurar e reportar periodicamente os **Indicadores Chave de Risco (KRIs)** à área de Controles Internos, Riscos e Compliance; e
- Implementar e executar os controles e **Planos de Ação** em seus processos, assegurando que sejam efetivos e resultem em redução do grau de **Exposição aos Riscos** a níveis aceitáveis.

Demais áreas

Todos os **Colaboradores**, independentemente do seu cargo, têm as seguintes responsabilidades:

- Cumprir a Estrutura Normativa Interna, a legislação e regulamentação aplicável;
- Reportar através do Canal de Ética e Conduta qualquer violação ou suspeita de violação a leis ou regulamentações aplicáveis, ou descumprimento da Estrutura Normativa Interna; e
- Apresentar todas as informações e/ou documentos corporativos dos quais estejam na posse, quando solicitados (i) pela Auditoria Interna, (ii) pela área de Controles Internos, Riscos e Compliance ou (iii) pela Comissão de Ética e Conduta, no contexto de investigação interna.

8. Aprovações

Nome / Cargo	Descrição
Marcos Corradi Gerente Executivo de Controles Internos, Riscos e Compliance	Elaboração/Revisão
Patricia Thomazelli Diretora Jurídica	Revisão
Gilsomar Maia Sebastião Vice-Presidente Adm. e Financeiro e Diretor de Relações com Investidores	Revisão
Dennis Herszkowicz CEO	Revisão
Comitê de Auditoria Estatutário	Recomendação
Conselho de Administração	Aprovação

ORGANIZATIONAL POLICY

Subject: Risk Management, Internal Controls and Compliance	**Identification:** PO-GC-03 **Version:** 05
Board in Charge: Internal Controls, Risks and Compliance	**Published on:** 05/05/2026
Related Rules:	**Review by:** 05/05/2029

1. Objective

The purpose of this policy is to establish the principles, guidelines, and responsibilities to be observed in the management of Corporate **Risks**, **Internal** Controls, and **Compliance**, as well as to promote a **Culture of Risk Management** and the **Integrity program** throughout all levels of TOTVS.

2. Scope

This Policy applies to all divisions of TOTVS, their respective employees and officers, as well as their wholly-owned subsidiaries; the rules set forth herein must be incorporated into the policies of direct and indirect subsidiaries, both in Brazil and in other countries, while always complying with their articles of incorporation and applicable local laws.

It must also be ensured that **Third parties**, subcontractors, representatives, consultants, suppliers, and service providers of any kind, when interacting with or representing TOTVS, also base their actions on the provisions of this Policy.

3. References

- ABNT (Brazilian National Standards Organization) NBR ISO 31000:2018: Risk Management — Principles and Guidelines.
- CODEC – TOTVS Code of Ethics and Conduct.
- Brazilian Code of Corporate Governance of Publicly-held Companies – Brazilian Institute of Corporate Governance – "IBGC".
- COSO ERM – Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework.
- Decree 11.129/22 – Decree regulating the Anti-Corruption Law.
- TOTVS Bylaws.
- IBGC: Corporate Governance, Corporate Risk Management and Compliance in the light of Corporate Governance booklets.
- Law 12.846/13 – Brazilian Anti-Corruption Law.
- CGU Ordinance 909 – Evaluation of integrity programs undertaken by legal entities.

4. Definitions

Action Plan: an action or set of actions aimed at mitigating or reducing the level of exposure to an identified risk; this may take the form of a project, a specific action, or a process control (ongoing action).
Annual Compliance Schedule: a plan designed to determine the prioritization of actions outlined in the Integrity Program.
Climate Change: refers to long-term changes in temperature and weather patterns, which may be caused by natural factors or result from human activities.

Compliance: derived from the English verb "to comply," which means conformity—that is, the duty to comply with and enforce laws, decrees, regulations, and instructions applicable to TOTVS's activities.
***Control Self-Assessment (CSA)*:** Control Self-Assessment is a methodology/technique used to evaluate the design and operational effectiveness of internal controls. It involves a questionnaire completed by business unit managers to self-assess both the internal controls and the risks associated with the processes under their responsibility.
Dictionary of Priority Risks: a standardized reference for identifying, categorizing, and organizing risk events that could affect the company's strategic objectives.
Employee or Employees: For the purposes of this Policy, this term refers to all employees who work at TOTVS.
Ethics and Conduct Hotline: a channel through which anyone who has a direct or indirect relationship with TOTVS (including employees, shareholders, customers, suppliers, franchisees, and partners, as well as their employees and any third parties) to confidentially report situations that may constitute a violation of the TOTVS Code of Ethics and Conduct or any other act that violates or may violate applicable laws and/or regulations.
Impact: refers to the result or consequence of a risk event occurring. The impact of the risk is analyzed in different areas, according to the defined rule.
Integrity Program: a set of internal integrity mechanisms designed to prevent, detect, and combat fraud, corruption, and other illegal acts committed in the private or public sectors, in accordance with applicable regulations in Brazil and/or abroad, in the locations where TOTVS operates.
Internal Controls: a set of manual and systemic activities and controls that form a protective barrier to ensure that operational activities and decision-making take place in a secure environment and that risks are quickly identified and addressed.
Internal Regulatory Framework: consists of regulatory documents that establish policies, standards, guidelines, rules, procedures, templates, and methods designed to guide Employees' interactions in their daily activities, in line with TOTVS's values, culture, and strategy, and in accordance with applicable regulations.
Key Risk Indicators (KRIs): indicators used to measure and monitor data associated with risks, either of a predictive/preventive nature if there are metrics indicating that they are likely to materialize, or a detectable nature, in the case of indicators showing that the risks have already materialized.
Opportunity: an event that can positively impact the undertaking of Company objectives, contributing to the generation and conservation of value.
Probability: qualitative or quantitative level that defines the likelihood of a risk event occurring.
Public Entities: any agency or entity directly or indirectly linked to any branch of the national or foreign public administration, such as, but not limited to, the Federal Government, the Federal District, the states, the municipalities, and the diplomatic missions of foreign countries. This concept also includes legal entities controlled by these bodies or entities, even if they are organized under private law, such as local government agencies, state-owned enterprises, foundations, associations, and international organizations.
Risk Appetite: refers to the level of risk the Company is willing to take to achieve its strategic objectives. The Company's Risk Appetite is defined and measured on a qualitative basis.
Risk Exposure: quantification of the likelihood that TOTVS will be affected by a particular risk.
Risk Factor: internal or external factor that may give rise to Risks.
Risk Management Culture: a set of accepted and practiced ethical standards, values, attitudes, and behaviors, and the integration of risk management into the decision-making process at all levels.
Risk matrix: consists of a graphical representation of the inventory of mapped risks, classified in quadrants according to their materialization probabilities and their impacts.
Risk Owner: responsible for the execution of internal controls to ensure that the risk is properly managed and for the definition and implementation of the necessary action plans for remediation and/or minimization of risks, as well as for the continuous monitoring and identification of new risks.

Risk tolerance: maximum level of exposure to risks that the entity is willing to incur in taking advantage of opportunities and pursuing and carrying out its strategy.
Risk: An event that could adversely affect TOTVS's results and its ability to achieve its strategic and business objectives.
Senior Management: members of the Board of Directors and the Executive Board.
Statutory Management: CEO and Vice Presidents of TOTVS.
Third Party(ies): any individual (other than an employee) or legal entity that has any relationship with TOTVS, including franchisees.
TOTVS or the Company: means TOTVS S.A., its subsidiaries and direct and indirect affiliates, individually or collectively, in Brazil or abroad, with the exception of TOTVS Techfin.

5. Guidelines

- TOTVS is committed to ethical conduct in its relationships with **Employees**, customers, partners, suppliers, investors, **Government Agencies**, and other stakeholders, and to compliance with applicable laws and regulations, including, but not limited to, anti-corruption laws and the Company's internal policies, standards, and procedures;
- The **Risk** management and Internal Controls process should provide input for decision-making aimed at mitigating or reducing the level of **Risk Exposure** and ensuring that actions are appropriately prioritized;
- The information used for **Risk** management and internal controls must be complete and accurate, reflecting the current status of TOTVS's operations;
- The Company's **Risks** must be communicated to all those involved in their management and monitoring, and reported in a timely manner.

The Internal Controls, Risk, and Compliance department reports directly to the CEO of TOTVS and enjoys the independence and autonomy necessary to carry out activities related to the **Integrity Program**, including unrestricted access to the information required to fulfill its responsibilities; these principles are reinforced by the support of TOTVS's senior management.

5.1. Risk Management

5.1.1. Risk Category

The Company classifies its **Risks** as described below, taking into account both external and internal factors.

Strategic Risk: Risk events associated with decisions that affect TOTVS Group's business strategy or strategic objectives, considering the internal and external environment.
Operational Risk: refers to potential losses resulting from disruptions, failures, deficiencies, or inadequacies in internal processes, personnel, the organizational environment, or technology, or caused by external events, including physical risks to facilities.
Financial Risk: This risk is associated with TOTVS's exposure to potential financial losses.
Regulatory/Compliance Risk: Risks of legal or regulatory sanctions, financial loss, or reputational damage that TOTVS may incur as a result of failure to comply with laws, agreements, regulations, the Code of Ethics and Conduct, and other requirements.
Information Technology Risks: Risks related to the information technology environment (including, but not limited to, infrastructure, access management, information security, and the use of artificial intelligence) that could impact TOTVS's business, such as cyberattacks, data breaches, IT system downtime, and technological obsolescence.

5.1.2. Risk Management Process and Methodology

The **Risk** management methodology applied at TOTVS is supported by a hybrid model that incorporates the components described in COSO ERM (*Enterprise Risk Management*) and ISO 31000. This approach establishes a framework for the integrated and continuous management of Corporate **Risks**, structured around six (6) essential stages, in addition to aspects of culture and governance, as detailed below:

5.1.2.1. Establishment of the Context

The initial stage of the process involves identifying and understanding strategic objectives, taking into account internal and external factors that may impact the achievement of these objectives over the short (1 year), medium (2 to 3 years), and long term (4 to 5 years), covering industry trends, technological changes, the macroeconomic landscape, the regulatory environment, sustainability issues, and climate change, as well as any other factors identified in the scenario analysis.

5.1.2.2. Risk Identification

The **Risk** identification process involves the use of specific tools, such as process mapping, interviews with managers responsible for each business area or segment and with senior management, as well as an analysis of past **Risk** events. This process should enable the identification of risks, with the aim of establishing risk matrices and keeping them constantly updated based on events that could impact TOTVS's strategic business objectives.

This step should also ensure a direct correlation between the identified **Risks** and TOTVS's material issues, taking into account financial and sustainability aspects, and using the **Dictionary of Priority Risks** as a standardized reference for categorization.

5.1.2.3. Risk Analysis and Assessment

Risks and their associated **Risk Factors** are assessed based on their **Probability** and **Impact**, taking into account the following areas:

- **Financial:** measures direct financial loss, taking into account the **Impact** on the company's operating results;
- **Reputational:** assesses the extent of negative exposure to TOTVS's image within its ecosystem (customers, partners, investors, and **Employees**) and the resulting impact on digital media or news outlets;
- **Legal/Compliance:** assesses the **Impact** of legal or regulatory sanctions, judicial or administrative proceedings, non-compliance with licenses or applicable laws, the Code of Ethics and Conduct, among other factors;
- **Operational:** measures the level of disruption to internal processes or the provision of services to customers, taking into account the time required to resume normal operations, including physical events that may impact operational continuity; and
- **Information Security:** assesses damage to the integrity, availability, and reliability of data belonging to TOTVS and its customers resulting from cyber incidents or data breaches.

For the consolidated classification of **Risk Probability** and **Impact**, the highest level of criticality identified for each of the analyzed **Risk Factors** shall prevail. The final risk rating is determined by plotting points on the **Probability** and **Impact** axes, resulting in four levels: (i) Low; (ii) Medium; (iii) High; and (iv) Critical. In addition, the analysis may consider the interconnectivity among the **Risks** in the matrix as a qualitative factor for understanding potential chain **Impacts**.

This document is the property of TOTVS. All rights reserved. ©
This document is the property of TOTVS. All rights reserved. ©

5.1.2.4. Risk Treatment

The definition of a risk response involves the development, formalization, and implementation of one or more **Action Plans** to mitigate **Risk** events by the respective responsible departments. The treatment should aim to reduce the **Probability** and/or **Impact** of the identified **Risks**, ensuring that the responses are effective and that resources are used optimally and in line with TOTVS's strategic objectives.

The treatment process is supported by potential enhancements to **Internal Controls** and the establishment of **Key Risk Indicators (KRIs)** linked to specific **Risks** or **Risk Factors**, with a single indicator capable of monitoring more than one event simultaneously. In cases where the indicator does not allow for the setting of quantitative targets, the assessment is based on a qualitative analysis of the trend and the indicator's historical performance.

Risks classified as High and Critical must be addressed through **Action Plans** aimed at lowering their classification, and such actions must be initiated within 60 days of the formalization of the respective plan. Structural plans for mitigating High and Critical **Risk** issues that depend on unavailable resources, highly complex IT projects, or organizational change may be granted extended deadlines, subject to the recommendation of the Vice President of the responsible division and approval by the Statutory Audit Committee. In this case, temporary compensatory controls must be implemented within 60 days, pending the completion of the final **Action Plans**.

TOTVS accepts the **Risks** when the company decides to maintain its current level of exposure without implementing new mitigation measures. This decision must comply with the approval authorities set forth below:

<table>
<tr><th rowspan="2">Risk Rating</th><th colspan="3">Risk assumption authority – TOTVS</th></tr>
<tr><th>Recommendation</th><th>Approval of Acceptance</th><th>Report/Data</th></tr>
<tr><td>Critical</td><td rowspan="2">Chief Executive Officer and Statutory Audit Committee</td><td rowspan="2">Board of Directors</td><td rowspan="2">-</td></tr>
<tr><td>High</td></tr>
<tr><td>Medium</td><td>Vice-president responsible for risk</td><td>Chief Executive Officer</td><td>Statutory Audit Committee</td></tr>
<tr><td>Low</td><td rowspan="2">Director or head responsible for risk</td><td rowspan="2">Vice-president responsible for risk</td><td rowspan="2">Chief Executive Officer</td></tr>
<tr><td>Very Low</td></tr>
</table>

5.1.2.5. Monitoring and Reporting

Proper **Risk** monitoring aims to ensure the effectiveness of the measures taken and timely communication to stakeholders, and is based on the following pillars:

- Ongoing monitoring of the Company's **Internal Control** environment through **Risk** mapping and controls;
- Implementation and monitoring of **Risk** response measures (**Action Plans** and/or controls), the effectiveness of which is tracked by the responsible departments with support from the Internal Controls, Risk, and Compliance department, which is responsible for reporting the consolidated status to TOTVS's Statutory Audit Committee; and
- Establishment and monitoring of **Key Risk Indicators (KRIs)**, defined by the departments responsible for **Risks** in conjunction with the Internal Controls, Risk, and Compliance department. KRIs support the assessment of risk levels **Probability** and **Impact** and the identification of the need for additional **Action Plans**, with the aim of keeping risks at levels deemed acceptable by TOTVS. The **KRIs** should be used by the **Risk Owners** to aid in decision-making and to strengthen the **Culture of Risk Management**.

Any extension of deadlines for the completion of **Action Plans** must be preceded by a formal justification from the responsible department and reported to the Statutory Audit Committee. In the case of **Risks** classified as High and Critical, the Statutory Audit Committee must inform the TOTVS Board of Directors of the reasons for the delay and the new estimated completion date for the relevant plans.

5.1.3. Risk Matrix Review and Evaluation Cycle

The **Risk Matrix** must be reviewed annually by the Internal Controls, Risk, and Compliance department, in accordance with the analysis criteria set forth in this policy, evaluated by the Vice Presidents and the Chief Executive Officer, and submitted for recommendation by the Statutory Audit Committee and for approval by the Board of Directors.

The **Risks** identified in the new **Matrix** must be addressed through **Action Plans** submitted to the Statutory Audit Committee, and their status regarding completion and analysis of changes in the **Risks** within the **Matrix** must be monitored on a quarterly basis The Internal Controls, Risk, and Compliance department is responsible for verifying the implementation of these **Action Plans**.

The Internal Controls, Risk, and Compliance department must also periodically report to the Statutory Audit Committee and the Board of Directors on the progress of the **Action Plans**, the **Key Risk Indicators (KRIs)** calculated, and the level of **Risk Exposure**. Presentations and reports must be included in the annual agenda of the Statutory Audit Committee and the Board of Directors, in accordance with the schedule established for each fiscal year.

5.2. Internal Controls

The internal control framework must be evaluated periodically to assess the effectiveness of existing **Internal Controls** and potential impacts arising from changes in the internal and/or external environment, taking into account: (i) the Company's strategic objectives; (ii) the composition and nature of the accounting accounts; (iii) the possibility of losses resulting from errors and fraud; and (iv) the complexity of transactions in the accounting accounts.

This document is the property of TOTVS. All rights reserved. ©
This document is the property of TOTVS. All rights reserved. ©

5.2.1. Stages of Internal Control Management

The Internal Controls, Risk, and Compliance department must map processes and controls, perform design tests ("walkthroughs"), and conduct effectiveness tests ("Control Tests") to confirm its understanding of the mapped processes and to verify that the controls are implemented and functioning properly.

Controls that are missing or deemed inadequate for mitigating the identified **Risks** are reported to the responsible departments so they can develop **Action Plans** aimed at reducing **Risk Exposure** and improving the control environment.

Once these steps have been completed, those responsible for the processes must conduct an annual Control Self-Assessment (Internal Controls Self-Assessment) in the system used by TOTVS and, where applicable, identify any new risks detected in their processes or activities.

The entire process of mapping and reviewing controls, along with the respective results, is reported to TOTVS's Statutory Audit Committee.

5.3. Compliance

5.3.1. Integrity Program

The **Integrity Program** aims to ensure that all **Employees** are familiar with and comply with applicable laws and regulations, as well as TOTVS's guidelines and rules of conduct, as well as ensuring that the **Third Parties** with whom the Company does business share the ethical principles adopted by TOTVS.

Every year, the Internal Controls, Risks and Compliance Department assesses the activities of each of the **Integrity Program** pillars with the goal of identifying improvements in its processes. This assessment is conducted by monitoring the program's results and indicators reported to the governing bodies during the previous cycle.

The TOTVS **Integrity Program** is structured around five pillars, as described below:

5.3.1.1. Integrity Culture

The purpose of this pillar is to strengthen and promote a culture that aligns with TOTVS's standards of ethics and integrity, through the ongoing engagement and support of TOTVS's senior management and key leaders.

5.3.1.2. Risk Assessment

This pillar aims to identify and assess the main **Risks** from an anti-corruption/**Compliance** perspective to which TOTVS is exposed, as well as measure their **Impacts** and recommend mitigation measures, taking into account compliance with applicable anti-corruption legislation and the conduct guidelines established in the Code of Ethics and Conduct and in the other Standards of the **Integrity Program**.

Compliance risks are reassessed annually by the Internal Controls, Risk, and Compliance department to monitor risks from the previous cycle and to identify and address any new risks that may have been identified.

5.3.1.3. Code of Ethics and Conduct, Policies and Procedures

The purpose of this pillar is to establish and formalize the internal guidelines, rules, and procedures that must be followed by **Employees** and **Third Parties** under the **Integrity Program**, thereby providing a framework for the implementation and/or optimization of integrity mechanisms and controls.

5.3.1.4. Communication and Training

The Communication and Training pillar aims to raise awareness and facilitate the development of a **Risk Management Culture**, as well as to ensure that **Employees** understand the guidelines, rules, and responsibilities they must adhere to under the TOTVS **Integrity Program**.

The Internal Controls, Risk, and Compliance department must develop and implement the Annual Communication and Training Plan, taking into account: (i) the relevance of the topics in light of the guidelines set forth in the Code of Ethics and Conduct and other regulatory documents; (ii) the target audience; (iii) frequency and available communication channels; and (iv) the need to reinforce topics identified in the history of events or questions related to the topic, if applicable.

The Annual Communication and Training Plan must be submitted for review and approval by the Statutory Audit Committee and the Board of Directors, the bodies responsible for overseeing the plan's implementation through reports from the Internal Controls, Risk, and Compliance department.

5.3.1.5. Detection and Remediation

This pillar aims to identify instances of improper or illegal conduct, fraud, or any other violations of applicable laws and regulations and TOTVS's Policies, as well as to ensure that such conduct is stopped and that disciplinary and/or corrective measures are taken, using as its primary tool an independent ("**Ethics and Conduct Channel**") for receiving and handling reports, available to internal and external stakeholders by calling **0800 721 5966** in Brazil and **+55 11 3232 0766** for other locations, or through the website: **https://www.canalconfidencial.com.br/totvs/.**

The **Ethics and Conduct Channel** is managed by the Internal Controls, Risks and Compliance Department, whose primary responsibilities is to (i) receive complaints for investigation by the responsible areas, according to the nature of the reports; (ii) investigate reports of bad conduct; and (iii) report the received complaints to the Ethics and Conduct Committee and other governance bodies as appropriate.

Cases of misconduct are reviewed by the TOTVS Ethics and Conduct Committee, and the Internal Controls, Risk, and Compliance department operates with functional independence and has access to the Committee's meetings, investigation data, and discussions regarding the management of consequences.

6. Consequence Management

In the event of non-compliance with this Policy or the other documents comprising the **Internal Regulatory Framework** and applicable laws and regulations, measures will be taken to address the resulting labor, civil, Criminal, and Administrative consequences that may apply to those responsible for the violations, including the possibility of termination for cause and termination of the contract for just cause in the case of franchisees and any **Third Parties** with whom there is a contractual relationship.

7.Assignments

Board of Directors

- Approve the Risk Management, Internal Controls and Compliance Policy;
- Approve TOTVS's strategic objectives, **Risk** management and **Internal Controls** methodology, and **Integrity Program**;
- Determine the appetite and **Risk Tolerance** levels proposed by the Board of Directors and recommended by the Statutory Audit Committee;
- Annually approve the **Priority Risk Matrix**, taking into account the respective management actions adopted and their results, as well as the **Key Risk Indicators (KRIs)** to be monitored;
- Approve the public information documentation regarding the **Risk** management model and the transparency of information provided to internal and external stakeholders;
- Ensure that adequate resources are available for the effective operation of the **Integrity Program** and guarantee the autonomy of the Internal Controls, Risk, and Compliance department;
- Approve the annual communication and training plan prepared by the Internal Controls, Risk, and Compliance department;
- Review and deliberate on the recommendations of the Statutory Audit Committee regarding the results of Risk Management, Internal Controls, and Compliance, as well as those of the **Integrity Program**; and
- Approve High and Critical **Risk** taking.

Statutory Audit Committee

- Review this Policy and any revisions thereto and submit a recommendation to the Board of Directors regarding its approval;
- Assist the Executive Board in defining the guidelines and methodology for managing **Risks** and **Internal Controls**, as well as the metrics for measuring **Risk Tolerance** and **Risk Appetite**, and submit its recommendation for approval to the Board of Directors;
- Evaluate risk management efforts and the development of the **Priority Risk Matrix**, and present its recommendations to the Board of Directors;
- Assess and recommend to the Board of Directors the establishment of risk appetite and **Risk Tolerance** levels;
- Monitor and periodically evaluate the results of control tests, the **Action Plans** for risk mitigation, and the **Key Risk Indicators (KRIs)** identified, reporting any deviations and incidents deemed relevant to the Board of Directors;
- Discuss and approve the **Annual Compliance Schedule**;
- Evaluate and monitor the **Action Plans** resulting from the audit of the **Integrity Program**;
- Report periodically to the Board of Directors any serious cases of misconduct related to this Policy, as well as any disciplinary measures taken; and
- Make recommendations to the Board of Directors regarding High and Critical **Risk** taking.

Ethics and Conduct Committee

- Monitor and evaluate the reports on the findings and investigations of complaints received through the TOTVS Ethics and Conduct Channel; and
- To determine the validity and severity of complaints regarding violations of the Code of Ethics and Conduct, applicable laws, and/or other internal TOTVS policies, and to recommend to the CEO the appropriate disciplinary action for cases received through the Ethics and Conduct Channel.

Board of Directors and Other Boards

- Conduct business practices that comply with applicable laws and regulations and with the **Internal Regulatory Framework**;
- Support the implementation of the **Integrity Program** and demonstrate commitment to it;
- Manage the **Risks** under their responsibility and assist in the development of controls and mitigation measures; and
- Ensure that TOTVS's code of conduct is communicated to and understood by partners, franchisees, distributors, customers, and other **Third Parties**.

Internal Controls, Risks and Compliance

- Propose amendments and submit this Policy for approval;
- Develop, implement, manage, and disseminate the **Risk** management methodology and the **Integrity Program**;
- Monitor and report on the **Action Plans** and the **Key Risk Indicators (KRIs)** defined for managing **Risks**;
- Raise awareness among managers and other **Employees** regarding the importance of **Risk Management**, **Internal Controls**, and the **Integrity Program**;
- Conduct annual **Internal Controls** in accordance with this policy;
- Act independently and autonomously to ensure impartiality in all activities, and report to the Chief Executive Officer and the Statutory Audit Committee if anything compromises their independence;
- Share with Internal Audit any information and/or facts that are the subject of an internal investigation;
- Manage the activities of the **Ethics and Conduct Channel** and report complaints to the Ethics Committee and other applicable governance bodies; and
- Report on **Risk Matrix** and the results of **Integrity Program** to the Statutory Executive Board, the Statutory Audit Committee, and the Board of Directors.

Internal Audit

- Assess the integrity of information, legal compliance, and the effectiveness of controls, ensuring the protection of assets and the alignment of processes with TOTVS's strategic and governance objectives;

- Assess the effectiveness of the organization's **Risk** management processes and mitigation plans;
- When prompted, investigate complaints received through the **Ethics and Conduct Channel** or by any other means;
- Share, if requested, with the Internal Controls, Risk, and Compliance department any nonconformities identified during the audit; and
- Ensure functional independence and technical objectivity, acting free from external interference and reporting any limitations on its autonomy directly to the Statutory Audit Committee.

Human Relations

- Promote and ensure that the principles of the **Integrity Program** are embedded in TOTVS's organizational culture.

Legal Board

- Advise TOTVS on regulations issued by regulatory agencies and on legislative changes at the federal, state, and municipal levels;
- Report any occurrence of an act constituting an administrative, civil, or criminal offense to the Executive Board and the Board of Directors of TOTVS; and
- Support the Internal Controls, Risks and Compliance area in the interpretation of applicable anti-corruption laws.

Risk Owners/Business and Operational Units

- Continuously identify and document the **Risks** under their management;
- Conduct an annual **Control Self Assessment** of the processes under your responsibility;
- Notify the Internal Controls, Risk, and Compliance department of any new **Risks** identified and any changes to your business processes;
- Implement, calculate, and periodically report the **Key Risk Indicators (KRIs)** to the Internal Controls, Risk, and Compliance department; and
- Implement and execute controls and **Action Plans** in your processes, ensuring that they are effective and result in reducing the level of **Risk Exposure** to acceptable levels.

Other functions

All **Employees**, regardless of their position, have the following responsibilities:

- Comply with the Internal Normative Structure, the applicable legislation and regulations;
- Use the Ethics and Conduct Channel to report any violation or suspected violation of applicable laws or regulations, or noncompliance with the Internal Regulatory Framework; and
- Present all information and/or corporate documents that they possess when requested (i) by the Internal Audit department, (ii) by the Internal Controls, Risk and Compliance department, or (iii) by the Ethics and Conduct Committee, in the scope of the internal investigation.

8. Approvals

Name / Title	Description
Marcos Corradi Executive Manager of Internal Controls, Risks and Compliance	Development and review
Patricia Thomazelli Legal Officer	Review
Gilsomar Maia Sebastião Vice President of Administration and Finance and Director of Investor Relations	Review
Dennis Herszkowicz CEO	Review
Statutory Audit Committee	Recommendation
Board of Directors	Approval