Certified Tester
Finance Testing (CT-FT)
Syllabus

v1.0

Internacional Software Testing Qualifications Board

Aviso de Direitos Autorais

Histórico de revisões

Versão	Data	Observações
v1.0	30/09/2025	Revisão alfa
v1.0	01/02/2026	Revisão da versão beta
v1.0	17/04/2026	Versão de lançamento

Índice

Sumário

Agradecimentos

Este documento foi formalmente aprovado pela Assembleia Geral do ISTQB® em 17 de abril de 2026

Foi elaborado por uma equipe do International Software Testing Qualifications Board: Florian Fieber (presidente), Richard Seidl (vice-presidente), Nishan Portoyan (product owner), Adam Roman, Ilia Kulakov, Julija Jankeviciene, Mantas Aniulis, Patricia McQuaid, Pavel Sharikov, Raunak Maskay, Renzo Cerquozzi, Webstar Ongaki, Mitko Mitev, Baris Sarialioglu.

A equipe agradece aos Conselhos Membros por suas sugestões e contribuições.

As seguintes pessoas participaram da revisão, comentários e votação deste syllabus: Adam Roman (CaSQB), Anna Petrosyan (ArmSTQB), Amanda Logue (CSTB), Andrew Pollner (ASTQB), Arda Ender Torçuk (BNTQB), Bíró Ádám (HTB), Claude Zhang (CSTQB), Dietmar Gehring (LTB), Erhardt Wunderlich (GTB), Ferdinand Gramsamer (STB), Florian Fieber (GTB), Gary Mogyorodi (Grupo de Trabalho do Glossário), Gergely Agnecz (HTB), Grzegorz Holak (PTB), Judy McKay (ASTQB), Laura Albert (HTB), Liang Ren (CSTQB), Lucjan Stapp (CaSQB), Mantas Aniulis (LTSTQB), Mattijs Kemmink (BNTQB), Meile Posthuma (BNTQB), Michael Humm (GTB), Mohammed Kamel Abu Thawabeh (JOSTQB), Péter Sótér (HTB), Ralf Pichler (STB), Renzo Cerquozzi (STB), Shun Tsunoda (JSTQB), Stephan Christmann (STB), Tal Pe'er (Grupo de Trabalho de Exames), Tanja Tremmel (GTB), Taz Daughtrey (ASTQB), Vinicius Pazutti Correia (DSTB), Walter Eder (ATB).

O BSTQB® agradece aos voluntários de seu grupo de trabalho de traduções (WG Traduções) pelo empenho e esforço na tradução deste material: Gabriel Nuevo, George Fialkovitz, Irene Nagase, Osmar Higashi, Paula de Oliveira, Stênio Viveiros, Thiago Cesar Andrade.

O BSTQB® também agradece aos ISTQB® Accredited Training Providers no Brasil que foram convidados a contribuir na revisão da tradução. No momento deste trabalho os seguintes provedores estavam credenciados: Conecteseaqui (conecteseaqui.com.br), Exseed (www.exseed.com.br), Iterasys (www.iterasys.com.br).

O BSTQB® também agradece às empresas brasileiras credenciadas no ISTQB® Partner Program no Brasil que foram convidados a contribuir na revisão da tradução. No momento deste trabalho as seguintes empresas estavam credenciadas: Deltapoint (www.deltapoint.com.br), Keeggo (www.keeggo.com), Venturus (www.venturus.org.br).

0 Introdução

0.1 Objetivo deste Syllabus

Este syllabus constitui a base para a certificação *ISTQB®Certified Tester – Finance Testing* (CT-FT). Ele destina-se a profissionais que trabalham em ou com sistemas financeiros e que estão envolvidos em testes de software e garantia da qualidade nesse domínio. O ISTQB® disponibiliza este syllabus para:

- Conselhos membros, para tradução para o idioma local e para credenciamento de provedores de treinamento. Os conselhos membros podem adaptar o syllabus às suas necessidades linguísticas específicas e modificar as referências para adequá-lo às publicações locais.
- Órgãos de certificação, para elaborar questões de exame em seu idioma local, adaptadas aos objetivos de aprendizagem deste syllabus.
- Provedores de treinamento, para produzir materiais de treinamento e determinar métodos de ensino adequados.
- Candidatos à certificação, para se prepararem para o exame de certificação (seja como parte de um curso de treinamento ou de forma independente).
- A comunidade internacional de engenharia de software e sistemas, para promover a profissão de testes de software e sistemas e como base para livros e artigos.

0.2 O ISTQB® Certified Tester – Finance Testing

A certificação ISTQB® Certified Tester – Finance Testing (CT-FT) destina-se a profissionais envolvidos em testes de software ou garantia da qualidade em instituições financeiras, empresas de tecnologia financeira (fintech) ou órgãos reguladores. É adequada, por exemplo, para testadores, analistas de negócios, desenvolvedores, responsáveis pela conformidade, auditores e reguladores que desejam compreender os requisitos específicos de testes e conformidade dos sistemas financeiros.

A certificação oferece uma extensão focada no domínio da qualificação de Nível Fundamental (CTFL), aprimorando a compreensão do candidato sobre temas regulatórios, de risco, dados, segurança, automação e performance específicos do setor financeiro.

0.3 Trajetória profissional para testadores

O esquema ISTQB®apoia profissionais de testes em todas as fases de suas carreiras, oferecendo conhecimento tanto em amplitude quanto em profundidade. Indivíduos que obtiverem a certificação ISTQB®Certified Tester - Finance Testing também podem se interessar pelos Níveis Avançados (Test Analyst, Technical Test Analyst and Test Management, Test Automation Engineer) e, posteriormente, pelo Nível Especialista (Test Management or Improving the Test Process). A vertente de Especialista oferece um aprofundamento em áreas que possuem abordagens de teste e atividades de teste específicas, por exemplo, em Agile Testing, AI Testing, ou Mobile App Testing, ou que agrupam conhecimentos de teste para determinados setores, como Gambling or Gaming ou Game. Visite www.istqb.org para obter as informações mais recentes sobre o esquema ISTQB® Certified Tester

0.4 Resultados de Negócio

Esta seção lista os resultados de negócio esperados de um candidato que tenha obtido a certificação Certified Tester - Finance Testing.

Uma pessoa com a certificação Certified Tester - Finance Testing pode...

BO1	compreender a estrutura do setor financeiro, suas instituições, sistemas e processos, e explicar os desafios específicos dos testes nesse domínio.
BO2	aplicar práticas de teste que garantam a conformidade com regulamentos e normas financeiras, assegurando que os requisitos de auditabilidade, rastreabilidade e documentação sejam atendidos.
BO3	aplicar testes baseados em riscos a sistemas financeiros, priorizando atividades de teste de acordo com riscos comerciais, técnicos e regulatórios.
BO4	compreender práticas de teste que determinam a precisão dos dados, a consistência dos dados e a proteção dos dados em todos os sistemas financeiros, incluindo o uso de técnicas de mascaramento e anonimização.
BO5	aplicar técnicas de teste funcionais e não funcionais tipicamente utilizadas no domínio financeiro, com ênfase especial em aspectos não funcionais, tais como performance, confiabilidade e segurança.
BO6	compreender o papel da automação de testes em ambientes financeiros e aplicar estratégias de automação de testes de forma eficaz tanto em sistemas legados quanto modernos, levando em consideração as restrições regulatórias.

(Veja o mapeamento completo no Apêndice B).

0.5 Objetivos de Aprendizagem o e Nível Cognitivo de Conhecimento

Os objetivos de aprendizagem apoiam os resultados de negócios e são utilizados para criar os exames Certified Tester - Finance Testing.

As questões do exame confirmarão o conhecimento de palavras-chave no nível K1 (veja abaixo) ou dos objetivos de aprendizagem no respectivo nível de conhecimento.

Os objetivos de aprendizagem específicos e seus níveis de conhecimento são apresentados no início de cada capítulo e classificados da seguinte forma:

- K1: Lembrar
- K2: Compreender
- K3: Aplicar

Mais detalhes e exemplos de objetivos de aprendizagem são fornecidos no Apêndice A.

Para todos os termos listados como palavras-chave logo abaixo dos títulos dos capítulos, o nome e a definição corretos do glossário do ISTQB®devem ser memorizados (K1), mesmo que não sejam explicitamente mencionados no objetivo de aprendizagem.

0.6 O Exame para Certified Tester - Finance Testing

O exame de certificação Certified Tester - Finance Testing será baseado neste syllabus. As respostas às questões do exame podem exigir o uso de material baseado em mais de uma seção deste syllabus. Todas as seções do syllabus são passíveis de avaliação, exceto a Introdução e os Apêndices. Normas e livros são incluídos como referências, mas seu conteúdo não é passível de avaliação, além do que está resumido no próprio syllabus a partir dessas normas e livros.

Consulte o documento Exam Structures and Rules V1.0 para obter mais detalhes sobre o exame Certified Tester - Finance Testing.

Para se qualificar para o exame de Certified Tester - Finance Testing (CT-FT), os candidatos devem possuir uma certificação válida de ISTQB® Certified Tester Foundation Level (CTFL).

A familiaridade com sistemas financeiros ou projetos de software na área financeira é benéfica, mas não obrigatória.

0.7 Credenciamento

Um Conselho Membro do ISTQB® pode credenciar provedores de treinamento cujo material didático siga este syllabus. Os provedores de treinamento devem obter as diretrizes de credenciamento junto ao Conselho Membro ou órgão responsável pelo credenciamento. Um curso credenciado é reconhecido como estando em conformidade com este syllabus e está autorizado a incluir um exame ISTQB® como parte do curso.

As diretrizes de credenciamento para este syllabus seguem as Diretrizes Gerais de Credenciamento publicadas pelo Grupo de Trabalho de Gestão de Processos e Conformidade.

0.8 Tratamento de Normas

Organizações internacionais de padronização, como IEEE e ISO, emitiram normas associadas a características de qualidade e testes de software. Tais normas são referenciadas neste syllabus. O objetivo dessas referências é fornecer um framework (como nas referências à ISO 25010 relativas a características de qualidade) ou fornecer uma fonte de informações adicionais, caso o leitor deseje. Observe que os syllabi[1] do ISTQB® utilizam os documentos de normas como referência. Os documentos de normas não se destinam a ser objeto de exame.

O syllabus faz referência a regulamentações financeiras internacionais, normas específicas de domínio e melhores práticas de testes de software. As principais fontes incluem:

- European Union's Revised Payment Services Directive 2 (PSD2), PCI DSS, Basiléia III / IV e outros frameworks regulatórios europeus
- ISO 20022 Serviços Financeiros – Esquema universal de mensagens para o setor financeiro
- ISO 25010 – Modelo de qualidade do produto (SQuaRE)
- Open Web Application Security Project (OWASP), ISO 27001 para segurança
- ISTQB® syllabi

Uma lista completa de referências pode ser encontrada no Capítulo 9.

0.9 Nível de detalhe

O nível de detalhe deste syllabus permite cursos e exames consistentemente internacionais. Para atingir esse objetivo, o syllabus consiste em:

- Objetivos instrucionais gerais que descrevem a intenção do Nível de Testes Financeiros
- Uma lista de termos que os alunos devem ser capazes de recordar

[1] Nota do BSTQB: plural de syllabus

- Objetivos de aprendizagem para cada área de conhecimento, descrevendo o resultado cognitivo a ser alcançado
- Uma descrição das palavras-chave, incluindo referências a fontes como literatura ou normas reconhecidas

O conteúdo do syllabus não descreve toda a área de conhecimento de testes de software; ele reflete o nível de detalhe a ser abordado nos cursos de treinamento para Certified Tester Finance Testing. Ele se concentra em abordagens de teste e técnicas de teste que podem ser aplicadas a todos os projetos de software relacionados a finanças, incluindo aqueles que seguem o desenvolvimento ágil de software. Este syllabus não contém objetivos de aprendizagem específicos relacionados a testes ágeis, mas discute como essas abordagens de teste e técnicas de teste se aplicam em projetos de desenvolvimento ágil de software e outros tipos de projetos.

O syllabus utiliza a terminologia (ou seja, o nome e o significado) dos termos usados em testes de software e garantia da qualidade de acordo com o Glossário do ISTQB®.

0.10 Como este syllabus está organizado

Existem seis capítulos com conteúdo passível de avaliação. No título principal de cada capítulo está especificada a duração do capítulo para estudo; a duração não é indicada abaixo do nível do capítulo. *Para cursos de treinamento com credenciamento, o syllabus exige um mínimo de 8,75 horas de instrução*, distribuídas pelos seis capítulos da seguinte forma:

- **Capítulo 1: 50 minutos – Introdução ao setor de serviços financeiros**
  - Recordar os principais objetivos dos testes financeiros
  - Resumir as características únicas e os requisitos técnicos de vários ambientes de teste financeiro
  - Identificar os principais sistemas financeiros e seus fluxos de trabalho testáveis associados
  - Explicar como o conhecimento da área é aplicado para mitigar desafios comuns de testes no setor financeiro
- **Capítulo 2: 80 minutos – Teste de conformidade**
  - Resumir os objetivos dos testes de conformidade e a relação entre suas principais abordagens de teste
  - Explicar a relevância dos principais regulamentos e normas financeiras para os testes
  - Relembrar as consequências da não conformidade com as regulamentações financeiras
  - Resumir as características únicas dos testes financeiros
  - Compreender os princípios e mecanismos de implementação da
  - o Validação da Conformidade no Ciclo de Vida (CACV) da entrega de software
- **Capítulo 3: 45 minutos – Testes baseados em riscos**
  - Explicar as principais categorias de risco em sistemas financeiros
  - Explicar os princípios dos testes baseados em riscos na área financeira
  - Explicar como a priorização baseada em risco afeta as atividades de teste em aplicativos financeiros
- **Capítulo 4: 90 minutos – Teste de dados e gerenciamento de dados**

- Explicar a importância da precisão e consistência dos dados em todos os sistemas financeiros
- Aplicar técnicas de reconciliação de dados aos processos financeiros do sistema de sistemas
- Explicar a importância da privacidade de dados e a proteção de dados nos testes financeiros

- **Capítulo 5: 165 minutos – Teste funcional e não funcional**
  - Aplicar testes funcionais para validar sistemas financeiros
  - Explicar os riscos de desempenho em sistemas financeiros durante períodos de pico
  - Aplicar testes de carga e testes de estresse em contextos específicos da área financeira
  - Explicar as necessidades de testes de segurança e de disponibilidade em sistemas financeiros
  - Explicar como a GenAI pode apoiar e melhorar os testes financeiros
- **Capítulo 6: 105 minutos – Automação de testes**
  - Papel da automação de testes nos testes financeiros
  - Explicar como a automação de testes contribui para a eficiência dos testes no setor financeiro
  - Estratégias de automação de testes
  - Aplicar estratégias de automação de testes em ambientes de TI financeiros legados e modernos
  - Desafios na automação de testes em ambientes regulamentados
  - Explicar os desafios da automação de testes em ambientes regulamentados
  - Desafios em diferentes tipos de automação de testes
  - Explicar os desafios da automação de testes em sistemas móveis, front-end e back-end

1 Introdução ao setor de serviços financeiros – 50 minutos

Palavras-chave

Palavras-chave específicas do setor

instituição financeira, norma regulatória

Objetivos de aprendizagem do Capítulo 1:

1.1 Fundamentos do teste de software em testes financeiros

FT-1.1.1 (K1) Recordar os principais objetivos dos testes financeiros

FT-1.1.2 (K2) Resumir as características únicas e os requisitos técnicos de vários ambientes de teste financeiros

FT-1.1.3 (K2) Identificar os principais sistemas financeiros e os fluxos de trabalho típicos com testabilidade associados a eles

1.2 Desafios e o papel do conhecimento de domínio nos testes financeiros

FT-1.2.1 (K2) Explicar como o conhecimento de domínio é aplicado para mitigar desafios comuns de teste no setor financeiro

Introdução ao Setor de Serviços Financeiros

O setor de serviços financeiros atua como o principal motor do comércio global, indo além da simples gestão de dinheiro para abranger um sofisticado ecossistema de bancos, seguros e investimentos. Nesse ambiente de alto risco, os sistemas de software não são apenas ferramentas, mas a própria infraestrutura da qual dependem a estabilidade econômica e a confiança do cliente. À medida que a transformação digital se acelera, o software que sustenta uma única instituição tornou-se indissociável da estabilidade da economia global. Essa convergência torna os testes rigorosos de software a única salvaguarda real contra um efeito dominó de falhas sistêmicas.

1.1 Fundamentos dos Testes de Software em Serviços Financeiros

1.1.1 Definição e Objetivos dos Testes Financeiros

O teste financeiro é o processo de verificação e validação de aplicativos de software utilizados no setor de serviços financeiros, incluindo bancos, tecnologia financeira (fintech), instituições financeiras não bancárias (NBFIs) — como seguradoras, fundos de pensão e empresas de leasing — e outros serviços financeiros especializados. Esses testes específicos do setor avaliam se os sistemas financeiros funcionam corretamente, com segurança e de acordo com a lógica de negócios e os requisitos regulatórios. Envolvem a validação de todo o ecossistema necessário para a execução de serviços financeiros, especificamente os fluxos de trabalho orientados por software que dão suporte a processos internos, interfaces do usuário externas e integrações com terceiros.

Os principais objetivos dos testes financeiros incluem:

- Correção funcional – verificar se as transações financeiras, cálculos matemáticos complexos (p. ex., taxas de juros, amortização) e saldos de contas são processados com regras de precisão e níveis de tolerância definidos para evitar perdas financeiras.
- Conformidade regulatória – verificar se o software está em conformidade com os requisitos legais globais e regionais exigidos e mitigar o risco de responsabilidade legal e penalidades financeiras.
- Garantia de integridade de dados – confirmação de que os registros de transações e os dados financeiros permanecem consistentes, precisos e intactos em todos os bancos de dados e sistemas integrados.
- Garantia de segurança – validação de que controles de segurança robustos estejam em vigor para proteger dados confidenciais de clientes e ativos financeiros contra ameaças cibernéticas, fraudes e acesso não autorizado.
- Resiliência operacional e performance – avaliar a estabilidade e a performance do sistema sob alta carga, validando a taxa de transferência e os tempos de resposta, e verificando os mecanismos de failover para manter a continuidade dos negócios.
- Confiança do cliente – gerando confiança de que o produto possui alta confiabilidade, protege os interesses dos usuários e preserva a reputação da instituição para apoiar a retenção de clientes a longo prazo.

1.1.2 Tipos de ambientes de teste financeiro em instituições financeiras

Os testes no setor financeiro podem ocorrer em vários tipos de ambientes técnicos, dependendo da arquitetura do sistema e do domínio de negócios. Os exemplos a seguir ilustram categorias comuns, e não uma lista exaustiva:

Ambiente omnicanal de consumo (banca de varejo e comercial). Esse ambiente prioriza uma jornada do cliente unificada e contínua em pontos de contato digitais e físicos integrados, incluindo aplicativos móveis, portais da web, agências, caixas eletrônicos (ATMs) e sistemas de resposta de voz interativa. Os objetivos dos testes concentram-se na avaliação da consistência da experiência da marca, da sincronização de dados entre os canais e da interoperabilidade entre as interfaces de front-end e os sistemas bancários centrais legados.

Ambiente de alto rendimento e baixa latência (investimento e negociação). Típicos de mecanismos de bolsa de valores e negociação algorítmica, esses ambientes devem processar milhões de transações por segundo com tempos de resposta inferiores a um milésimo de segundo. O teste de performance é a principal preocupação, com foco no rendimento, na latência mínima e no determinismo de execução para dar suporte ao processamento de volumes massivos com velocidade consistente.

Ambiente de API com alta densidade lógica e resiliência (fintech).

Os sistemas de fintech utilizam arquitetura de microsserviços para gerenciar lógica de negócios complexa por meio de entradas de alta dimensão. Os testes se concentram na resiliência operacional, garantindo que as falhas sejam isoladas para evitar impactos em cascata nos serviços dependentes. A validação requer a simulação de fluxos de trabalho de transações complexos, o que pode ser alcançado por meio de testes baseados em modelos, virtualização de serviços ou orquestração de testes orientada por IA.

Ambiente de mensagens orientado por esquemas (sistemas interbancários especializados). Esse ambiente facilita a comunicação interbancária usando padrões como ISO 20022 e protocolos como FIX (Financial Information Exchange). As atividades de teste enfatizam a validação do esquema para tipos de mensagens, incluindo relatórios PAIN (iniciação de pagamento), PACS (transferências de crédito) e CAMT (gestão de caixa).

Ambiente dependente do tempo e atuarial (seguros e hipotecas). Com foco no ciclo de vida de longo prazo de apólices e empréstimos, esses ambientes validam modelos matemáticos complexos para classificação de prêmios, avaliação de risco e amortizações de juros compostos. As principais preocupações de teste incluem a precisão em cálculos multivariáveis e **testes de viagem no tempo** — uma técnica de teste na qual o relógio do sistema ou o tempo simulado é intencionalmente modificado para verificar o comportamento correto da funcionalidade dependente do tempo.

1.1.3 Arquiteturas de sistemas financeiros e fluxos de trabalho com alta testabilidade

A arquitetura de uma instituição financeira é tipicamente composta por várias camadas interconectadas, cada uma apresentando preocupações distintas em relação aos testes:

- **Os sistemas bancários centrais** atuam como a infraestrutura centralizada para o processamento de transações financeiras, a manutenção de registros de clientes e a gestão de contas. Testar esses sistemas exige abordar complexidades arquitetônicas específicas, dependências transacionais e requisitos não funcionais críticos.
- **A camada de integração e middleware** funciona como a infraestrutura de interconexão que liga as interfaces front-end. Os testes se concentram na verificação da troca confiável de dados financeiros, na manutenção da integridade dos dados entre subsistemas e no isolamento de falhas para evitar um impacto em cascata nos serviços dependentes.
- **O front-end digital e os canais** incluem aplicativos móveis, portais da web e terminais de caixas eletrônicos ou pontos de venda (POS). A cobertura aborda o comportamento entre dispositivos, a autenticação biométrica, a estabilidade offline e o roteamento correto das transações, com arquiteturas de interface do usuário independentes de dispositivo que exigem renderização consistente em todas as plataformas de destino.

Os fluxos de trabalho testáveis em finanças incluem:

- **Fluxos de trabalho transacionais.** Os testes de transações financeiras concentram-se na verificação do ciclo de vida completo de uma instrução de pagamento em vários subsistemas. O escopo inclui transições corretas de estado , lógica de liquidação e comportamento de reversão tanto em condições normais de processamento quanto em condições de falha.
- **Fluxos de trabalho de conformidade e identidade**. A integridade da integração de clientes é mantida por meio da verificação de mecanismos de comprovação de identidade, incluindo autenticação de documentos e testes biométricos, de acordo com os padrões regulatórios Know Your Customer (KYC). Os fluxos de trabalho de contra lavagem de dinheiro (Anti-Money Laundering - AML) são avaliados para confirmar a detecção precisa de atividades suspeitas e a triagem eficaz de entidades em relação a listas globais de sanções, ao mesmo tempo em que se controlam as taxas de falsos positivos.
- **Fluxos de trabalho de investimento e tesouraria.** Teste de sistemas de investimento envolve validar o ciclo de vida completo da negociação — desde o roteamento de ordens no OMS/EMS (Order Management System/Execution Management System) até a liquidação final — em diversos tipos de ordens e bolsas globais. Isso requer verificação especializada para lógica específica de ativos, como modelos de precificação de derivativos e “kill switches” de risco algorítmico, juntamente com testes de performance rigorosos para latência e métricas de risco em tempo real.
- **Fluxos de trabalho operacionais e de back-office.** A cobertura do fluxo de trabalho operacional aborda a integridade da reconciliação, garantindo um fluxo consistente de dados de transações dos sistemas de front-office para o Razão e o alinhamento com registros externos. A cobertura inclui ciclos de processamento periódicos — como Fim do Dia, Fim do Mês e Fim do Ano — para validar a precisão da liquidação, relatórios fiscais e a manutenção de trilhas de auditoria completas para governança e conformidade.
- **Fluxos de trabalho especializados em seguros.** A cobertura do ciclo de vida das apólices concentra-se em transições de estado corretas e no cálculo preciso de prêmios com base em regras de subscrição e de risco. Os fluxos de trabalho de sinistros são projetados para facilitar a adjudicação sistemática, acionar protocolos de detecção de fraudes e executar liquidações. Esses processos exigem troca consistente de dados entre os principais sistemas de seguros para manter a integridade dos dados.

1.2 Desafios e o Papel do Conhecimento de Domínio nos Testes Financeiros

No setor de serviços financeiros, as habilidades genéricas de teste de software são frequentemente insuficientes devido à complexidade da base de teste, à precisão exigida no processamento de transações e à severidade das restrições regulatórias. O conhecimento de domínio funciona como um facilitador crítico para mitigar os seguintes desafios específicos de teste associados aos sistemas financeiros:

- Resolução do problema do oráculo de teste . Um dos principais desafios nos testes financeiros é o problema do oráculo de teste, em que determinar o resultado esperado correto para uma determinada entrada não é tarefa trivial devido aos complexos modelos matemáticos subjacentes (p. ex., precificação de derivativos, cálculos atuariais de risco ou curvas de rendimento). O conhecimento especializado na área permite a dedução independente dos resultados esperados para verificar a correção funcional.
- Tradução de mandatos regulatórios em condições de teste . As regulamentações financeiras são frequentemente abstratas e abertas a interpretações, dificultando a tradução direta em casos de

teste executáveis . A fluência no domínio permite que os testadores decomponham textos jurídicos de alto nível em critérios de aceite precisos e testáveis .

- Dependências de dados. As entradas financeiras possuem dependências rígidas entre campos de dados (p. ex., um tipo específico de transação que requer um código fiscal distinto). O conhecimento do domínio permite a definição dessas restrições para gerar dados de teste válidos que sejam aprovados na lógica de validação inicial do sistema.
- Validação de ciclos de vida de transações de ponta a ponta. As transações financeiras frequentemente atravessam vários sistemas heterogêneos, passando dos canais de entrega do front-office, passando pelos mecanismos de liquidação do middle-office até os livros contábeis gerais do back-office. Manter a integridade dos dados e a consistência de estado entre esses sistemas é um dos principais desafios de teste. A expertise no domínio é aplicada para verificar o ciclo de vida completo da transação, determinando que:
    - as transações sejam corretamente capturadas e validadas no ponto de entrada,
    - a consistência dos dados permanece intacta à medida que os dados passam por processos como compensação, liquidação ou conversão de moeda entre diferentes sistemas,
    - o estado final da transação seja refletido com precisão nos registros contábeis, trilhas de auditoria e componentes de relatórios.
- Priorização eficaz em testes baseados em riscos . Devido a restrições de tempo e altos volumes de testes de regressão, testes exaustivos são impossíveis. A avaliação genérica de risco pode falhar em identificar modos de falha financeira de alto impacto. O conhecimento especializado no domínio facilita a análise de impacto precisa. Os testadores podem distinguir entre defeitos cosméticos e falhas críticas que poderiam levar a perdas financeiras, multas regulatórias ou danos à reputação.

2 Teste de Conformidade – 80 minutos

Palavras-chave

auditabilidade, conformidade, validação contínua e automatizada da conformidade, testes de controle, testes negativos, testes substantivos, rastreabilidade

Palavras-chave específicas do setor

conformidade regulatória, General Data Protection Regulation (GDPR), Lei Sarbanes-Oxley (SOX), Digital Operational Resilience Act (DORA)

Objetivos de aprendizagem do Capítulo 2:

2.1 Objetivos e abordagens dos testes de conformidade

FT-2.1.1 (K2) Resumir os objetivos dos testes de conformidade e a relação entre suas principais abordagens de teste

2.2 Regulamentações financeiras e seu impacto nos testes

FT-2.2.1 (K2) Explicar a relevância dos principais regulamentos e normas financeiras para os testes

FT-2.2.2 (K1) Relatar as consequências da não conformidade com as regulamentações financeiras

2.3 Características distintivas dos testes em finanças regulamentadas

FT-2.3.1 (K2) Resumir as características únicas dos testes financeiros

2.4 Auditabilidade e validação contínua e automatizada da conformidade

FT-2.4.1 (K2) Compreender os princípios fundamentais da auditabilidade em testes de conformidade

FT-2.4.2 (K2) Compreender os princípios e mecanismos de implementação da Continuous Automated Compliance Validation (CACV) na conformidade no ciclo de vida de entrega de software

Teste de Conformidade

À medida que o software se torna a espinha dorsal da infraestrutura financeira global, a interseção entre engenharia e supervisão jurídica tornou-se uma fronteira operacional crítica. Este capítulo explora a rigorosa estrutura do teste de conformidade, uma disciplina que vai além da detecção tradicional de defeitos para se concentrar na integridade institucional e na adesão regulatória. Ao examinar as metodologias especializadas, os requisitos não funcionais obrigatórios e a evolução em direção à auditabilidade automatizada e contínua, definimos como os sistemas modernos mantêm a confiança em um ambiente legislativo cada vez mais escrutinado e complexo.

2.1 Objetivos e abordagens dos testes de conformidade

O teste de conformidade (também conhecido como teste de conformidade regulatório) é o processo de teste para determinar se um componente ou sistema está em conformidade com normas, leis, regulamentos e contratos definidos. Embora seja frequentemente categorizado como teste não funcional, no setor financeiro envolve frequentemente a validação da lógica de negócios funcional e dos dados em relação a mandatos regulatórios específicos. Ele avalia se as atividades, transações financeiras e informações estão em conformidade, em todos os aspectos relevantes, com as autoridades e critérios que regem a entidade auditada.

Os principais objetivos do teste de conformidade incluem:

- verificação da adesão – para obter garantia razoável de que o sistema e suas transações subjacentes estejam em conformidade com os frameworks regulatórios relevantes e políticas internas,
- identificação de risco – para identificar e avaliar os riscos de não conformidade material, garantindo que violações de mandatos legais ou regulatórios sejam detectadas precocemente para mitigar possíveis penalidades, perdas financeiras ou danos à reputação,
- validação dos controles – para avaliar a efetividade dos sistemas de controle interno na prevenção, detecção e correção de casos de não conformidade,
- apresentação de evidências – para gerar evidências de auditoria suficientes, relevantes e de alta confiabilidade que demonstrem a devida diligência e a adesão às normas para os stakeholders e os órgãos reguladores.

Os testes de controle e os testes substantivos representam duas abordagens complementares de teste utilizadas para garantir a conformidade:

- Os testes de controle avaliam se os controles internos foram projetados adequadamente e operam de forma eficaz para prevenir, detectar ou corrigir distorções materiais ou casos de não conformidade. O objetivo principal dos testes de controle é obter evidências de que os controles operam conforme o previsto, são aplicados de forma consistente e permanecem eficazes durante o período em revisão. Os testes de controle concentram-se nos processos e mecanismos, tais como fluxos de trabalho de aprovação, segregação de funções, controles de acesso e regras de validação automatizadas, ao invés dos resultados de transações individuais.
- Os testes substantivos consistem em procedimentos concebidos para detectar distorções materiais ou incumprimento através da análise direta de transações, saldos de contas e resultados. O objetivo principal dos testes substantivos é verificar a exatidão, integridade e validade dos dados e resultados produzidos pelo sistema. Ao contrário dos testes de controle, que validam a forma como o processamento é realizado, os testes substantivos validam o que o sistema produz, independentemente da existência ou efetividade dos controlos.

2.2 Regulamentos Financeiros e seu Impacto nos Testes

2.2.1 Principais regulamentações financeiras e sua relevância para os testes

O panorama de conformidade no setor financeiro é moldado por regulamentos, normas e diretrizes em diferentes níveis jurisdicionais. Alguns são juridicamente vinculativos, enquanto outros orientam as melhores práticas do setor. Sua prioridade depende do status legal e do potencial impacto nos negócios. A Tabela 1 fornece uma visão geral estruturada das principais regulamentações financeiras e sua relevância para os testes:

Tabela 1. Visão geral estruturada das principais regulamentações relevantes para sistemas financeiros e sua relevância para os testes

Área de foco	Regulamentação	Impacto da conformidade nos testes
Proteção de dados e privacidade	General Data Protection Regulation (GDPR) Lei Geral de Proteção de Dados (LGPD)	Verificar o tratamento lícito por meio do gerenciamento do consentimento, dos direitos dos titulares de dados, dos controles de acesso e da privacidade desde a concepção; utilizando PII (Personally *Identifiable Information*) mascaradas/sintéticas e respeitando os limites de retenção e jurisdição.
Transparência financeira	Lei Sarbanes-Oxley (SOX)	Validar os controles internos por meio da segregação de funções, fluxos de trabalho de aprovação, registros de auditoria imutáveis e histórico financeiro preservado utilizando conjuntos de dados submetidos à anonimização.
Segurança de pagamentos	Payment Card Industry Data Security Standard (PCI DSS)	Confirmar a proteção dos dados dos titulares de cartões por meio de encriptação, autenticação forte e fluxos de transações seguros, utilizando apenas *Primary Account Numbers* (PAN) tokenizados e registros mascarados
Resiliência operacional	Digital Operational Resilience Act (DORA)	Avaliar a resiliência das *information and communication technology* (ICT) por meio de planos de recuperação de desastres e continuidade de negócios (DR/BCP), failover e testes baseados em cenários, utilizando conjuntos de dados replicados e submetidos à anonimização.
Pagamentos e open banking	Payment Services Directive 2 (PSD2)	Verificar se as operações de open banking são seguras, testando a *Strong Customer Authentication* (SCA), a *Multi-Factor Authentication* (MFA), a segurança da *Application Programming Interface* (API) e o gerenciamento do ciclo de vida do consentimento utilizando contas sintéticas.
Capital bancário e risco	Basiléia III/IV	Apoiar a conformidade com a adequação de capital, validando modelos de risco de crédito, de mercado e de liquidez por meio de testes de estresse e testes baseados em cenários, utilizando grandes carteiras mascaradas ou sintéticas.
Combate à lavagem de dinheiro	Fifth and Sixth EU Anti-Money Laundering Directives (AMLD5/AMLD6)	Verificar os controles contra lavagem de dinheiro por meio de fluxos de KYC, triagem de sanções, geração de alertas e lógica de sinalização de risco utilizando padrões sintéticos realistas de clientes e transações.
Criptoativos	Markets in Crypto-Assets (MiCA) Regulation	Validar a conformidade de criptoativos testando salvaguardas de custódia, integridade de ordens e detecção de abuso de mercado utilizando carteiras sintéticas e transações criptográficas submetidas à anonimização.

As regulamentações financeiras variam entre regiões e jurisdições, exigindo a adaptação de frameworks de conformidade, mecanismos de controle e padrões de relatório dentro do processo de teste.

2.2.2 Consequências da não conformidade

A falha no cumprimento dos requisitos regulatórios e de conformidade no setor financeiro pode levar a consequências significativas nas dimensões financeira, jurídica, reputacional e operacional:

- **Multas financeiras e impacto econômico.** Os órgãos reguladores têm autoridade para impor multas monetárias substanciais e penalidades financeiras por não conformidade. Essas multas podem estar relacionadas a violações das regras contra lavagem de dinheiro, leis de privacidade do dado ou relatórios incorretos de acordo com as diretivas financeiras.
- **Sanções legais e regulatórias.** A não conformidade também pode desencadear ações de fiscalização além de penalidades monetárias, como ações judiciais, responsabilidade criminal, reestruturação obrigatória ou a nomeação de uma administração externa. Em casos de severidade, os reguladores podem impor medidas de fiscalização, como reestruturação obrigatória de ativos ou a nomeação de uma administração externa.
- **Prejuízo à reputação e à posição no mercado.** Incidentes de não conformidade podem prejudicar significativamente a confiança do público e dos stakeholders, resultando em cobertura negativa da mídia, preocupação dos investidores e perda de clientes.
- **Interrupção dos negócios.** Falhas de conformidade podem desencadear suspensões de serviços, restrições de licenças ou intervenção regulatória. Isso pode levar a perdas de receita, queda na participação de mercado e erosão da lealdade do cliente. Em casos de severidade, os reguladores podem impor medidas coercitivas, como reestruturação obrigatória de ativos ou a nomeação de uma administração externa.
- **Riscos operacionais e dívida técnica.** A não conformidade gera riscos operacionais sistêmicos e dívida técnica, prejudicando a estabilidade e a manutenibilidade dos sistemas de software. A falha na implementação dos controles de segurança exigidos expõe as organizações a vulnerabilidades de segurança, incluindo violações de dados e fraudes.

Esses riscos ressaltam a importância de integrar a validação da conformidade às atividades de desenvolvimento e teste de software.

2.3 Características Distintas dos Testes em Sistemas Financeiros Regulamentados

Os testes em sistemas financeiros regulamentados apresentam características distintas que influenciam significativamente a forma como o processo de teste é executado e controlado:

- **Testes impulsionados por mudanças regulatórias** . Os testes são frequentemente desencadeados por mandatos legislativos externos, em vez de objetivos comerciais internos. Ao contrário do desenvolvimento geral de software, onde os requisitos evoluem com base no feedback do mercado, os sistemas financeiros devem se adaptar a um fluxo contínuo de regulamentações novas e atualizadas. Esse cenário regulatório dinâmico requer uma estratégia de teste caracterizada por adaptação contínua, análise rigorosa de impacto e resposta rápida para manter a conformidade legal contínua.
- **Análise de requisitos com foco regulatório** é o processo especializado de identificar, interpretar e mapear mandatos legais e de conformidade em especificações de software com nível de testabilidade. Ao contrário da engenharia de requisitos padrão, que se concentra na utilidade comercial, esse processo prioriza a adesão a regulamentações externas e políticas de governança interna.
- **Teste negativo como uma necessidade regulatória**. Os sistemas financeiros devem resistir ativamente ao uso indevido, falhas e comportamentos não conformes. Os testes negativos

ajudam a identificar fraquezas de segurança, caminhos de fraude e lacunas lógicas ao testar entradas que parecem válidas, mas são proibidas. Isso verifica se o sistema bloqueia corretamente o acesso não autorizado, limita violações e infracções de regras regulatórias, como controles de sanções.

- **Gerenciamento de dados de teste críticos para a conformidade** . O gerenciamento de dados de teste é regido por regulamentações legais que restringem fundamentalmente a forma como os testes são realizados, distinguindo-o de setores não regulamentados, onde dados de produção podem ser copiados para fins de teste (ver Capítulo 4).
- **Testes baseados em evidências** caracterizam-se pela coleta, retenção e gerenciamento sistemáticos de testware para satisfazer auditores externos e órgãos regulatórios. O objetivo principal passa da detecção de defeitos para a demonstração de diligência devida e a validação de que controles específicos são executados de forma eficaz.
- **Os testes não funcionais obrigatórios** são uma atividade compulsória impulsionada por frameworks legais, estabelecendo a conformidade como uma característica de qualidade integrada, em vez de uma preferência comercial. Isso ajuda a mitigar vulnerabilidades de segurança que poderiam levar a fraudes financeiras ou violações de dados. Testes de eficiência de performance e confiabilidade são exigidos para verificar a estabilidade do sistema sob cargas de transações de alta frequência e para confirmar a resiliência operacional por meio de rigorosa validação de recuperação de desastres e continuidade de negócios.

2.4 Auditabilidade e Validação Contínua e Automatizada da Conformidade

2.4.1 Auditabilidade

A auditabilidade no contexto do teste de conformidade envolve a capacidade de reconstruir, revisar e verificar de forma independente as atividades de teste e os comportamentos do sistema sob teste (SUT). Ela abrange não apenas a verificação funcional do software, mas também a documentação rigorosa do próprio processo de teste. Essa documentação fornece evidências para que os reguladores verifiquem a execução efetiva dos controles regulatórios e confirmem que o sistema opera dentro dos limites legais e contratuais definidos.

Os principais componentes da auditoria incluem:

- **Rastreabilidade bidirecional** . A auditabilidade requer o estabelecimento de uma linhagem verificável que conecte mandatos regulatórios de alto nível a artefatos técnicos específicos. Esse componente permite vincular cada requisito regulatório aos casos de teste correspondentes (rastreabilidade para frente) e rastrear cada defeito ou resultado do teste de volta à regra regulatória ou ao objetivo de controle ao qual se refere (rastreabilidade para trás).
- **Retenção imutável de evidências**. O teste de conformidade exige a coleta e a preservação sistemáticas de testware. Isso inclui planos de teste, requisitos aprovados, registros detalhados de execução e capturas de tela de etapas críticas. Esses artefatos devem ser armazenados em um formato à prova de adulteração para servir como evidência irrefutável de diligência devida.
- **Integridade das evidências e privacidade** . Os sistemas devem gerar trilhas de auditoria seguras e com registro de data e hora que registrem todas as atividades do usuário, eventos de acesso e estados das transações. Esses registros devem ser protegidos contra alterações não autorizadas para servir como evidência legal válida durante investigações forenses ou revisões regulatórias. Fundamentalmente, ao capturar esses metadados, o processo deve incorporar técnicas de mascaramento de dados para evitar que informações financeiras confidenciais sejam

expostas na trilha de auditoria, apoiando assim a conformidade com as regulamentações globais de privacidade.

- **Reprodutibilidade** . A auditabilidade exige que os processos de teste e os comportamentos do sistema sejam reproduzíveis. O sistema deve capturar dados de configuração ambiental e parâmetros de entrada suficientes para permitir que um auditor independente reexecute um teste ou reproduza uma transação e obtenha o mesmo resultado. Essa capacidade confirma que os controles de conformidade operam de forma consistente e não estão sujeitos a variáveis transitórias ou não documentadas.

2.4.2 Validação Contínua e Automatizada da Conformidade

A Validação contínua e Automatizada da Conformidade (CACV - Continuous Automated Compliance Validation) é a prática de incorporar controles regulatórios e de segurança programaticamente ao longo de todo o ciclo de vida de entrega de software. Ao contrário dos modelos de auditoria tradicionais, que dependem de avaliações periódicas e pontuais, a CACV emprega a automação de testes para fornecer garantia contínua e em tempo real da conformidade regulatória. Essa abordagem transforma a conformidade de uma atividade de verificação reativa e manual em um recurso proativo e integrado à arquitetura do sistema.

Mecanismos de implementação

O CACV depende de implementações técnicas específicas para aplicar e monitorar os requisitos regulatórios:

- **Conformidade como Código** (CaC). Os requisitos regulatórios são traduzidos em código ou scripts legíveis por máquina. Isso permite que as regras de conformidade sejam controladas por versão, testadas e executadas automaticamente em relação à infraestrutura e ao código da aplicação.
- **Integração de pipeline e portas de qualidade**. As verificações de conformidade são integradas diretamente no pipeline de Integração Contínua/Implantação Contínua (CI/CD) . São estabelecidas “portas de conformidade” para bloquear automaticamente a promoção de código não conforme para ambientes de produção.
- **Monitoramento Contínuo de Controle** (CCM): Além da fase de compilação, o CACV envolve o monitoramento contínuo do ambiente de produção para detectar “desvios”. O desvio de configuração ocorre quando um sistema em conformidade é alterado após a implantação (p. ex., uma porta de firewall é aberta manualmente), tornando-o não conforme.

O fluxo de trabalho do CACV integra a verificação regulatória ao ciclo de vida de entrega de software por meio de quatro fases iterativas:

- **Elaboração e definição**. Os frameworks regulatórios são analisados para derivar requisitos precisos e testáveis. Estes são agrupados em perfis de conformidade para estabelecer critérios específicos para o software em teste.
- **Desenvolvimento**. Os requisitos de conformidade são implementados como código executável. Casos de teste funcionais são desenvolvidos e mapeados explicitamente às regras regulatórias para estabelecer rastreabilidade bidirecional entre requisitos e produtos de trabalho de teste.
- **Execução e inspeção automatizadas**. Testes de conformidade automatizados são executados continuamente no pipeline de CI/CD. Os controles de qualidade garantem o cumprimento das normas, impedindo que artefatos não conformes sejam promovidos para ambientes de produção.
- **Avaliação e relatórios**. Os resultados dos testes são avaliados para gerar evidências de auditoria imutáveis e relatórios de violação. O monitoramento contínuo detecta desvios de

configuração na produção, acionando fluxos de trabalho de correção para restaurar a conformidade.

3 Testes Baseados em Riscos – 45 minutos

Palavras-chave

risco, mitigação de risco, avaliação de risco, testes baseados em riscos, matriz de rastreabilidade

Palavras-chave específicas do domínio

Risco de conformidade, avaliação dinâmica de risco, aceite de riscos, prevenção de riscos, transferência de riscos

Objetivos de aprendizagem do Capítulo 3:

3.1 Categorias de Risco em Sistemas Financeiros

FT-3.1.1 (K2) Explicar as principais categorias de risco em sistemas financeiros

3.2 Princípios de Testes Baseados em Riscos em Finanças

FT-3.2.1 (K2) Explicar os princípios dos testes baseados em riscos em finanças

3.3 Atividades Baseadas no Risco

FT-3.3.1 (K2) Explicar como a priorização baseada em risco afeta as atividades de teste em aplicações financeiras

Introdução aos Testes Baseados em Riscos em Sistemas Financeiros

Os testes baseados em riscos são uma abordagem estratégica de teste de software que prioriza os esforços de teste com base nos riscos identificados associados a diferentes recursos ou funcionalidades de um aplicativo de software, calculados como o produto da probabilidade de falha e do impacto potencial nos negócios. Exemplos incluem falhas no cumprimento de normas (p. ex., GDPR, LGPD PSD2, PCI DSS ou MiCA) ou cálculos de risco ou modelos financeiros com defeitos. Os testes baseados em riscos são abordados na Seção 5 do Syllabus do Nível Fundamental do ISTQB [ISTQB_CTFL_SYL].

3.1 Categorias de Risco em Sistemas Financeiros

No setor financeiro, os riscos são identificados em três dimensões principais:

- **Riscos de negócio e financeiros**. Estes podem incluir riscos associados à migração de dados confidenciais, defeitos no tratamento de dados, cálculos incorretos e aplicação incorreta de regras.
- **Riscos técnicos e operacionais**. Estes incluem o aumento do escopo, suporte inadequado às ferramentas ou riscos mais específicos de dependência técnica, como a dependência excessiva de ferramentas específicas, frameworks de automação de testes ou APIs.
- **Riscos regulatórios e de conformidade**. Existem riscos relacionados a fornecedores e terceirização, como prestadores de serviços terceirizados que não cumprem obrigações de conformidade, segurança ou performance (especialmente relevante no âmbito da DORA). Podem ocorrer atrasos ou mal-entendidos na implementação de novos requisitos legais ou de conformidade. Esses riscos também se aplicam a sistemas desenvolvidos internamente.

O syllabus do ISTQB® Nível Fundamental distingue entre riscos de projeto e riscos de produto.

Os **riscos de projeto** estão relacionados à gestão e ao controle do projeto e podem afetar seu cronograma, orçamento ou escopo, prejudicando assim sua capacidade de atingir seus objetivos.

Os **riscos de produto** estão relacionados às características de qualidade do produto. Os riscos de produto podem incluir cálculos incorretos de empréstimos comerciais ou o não cumprimento dos protocolos aplicáveis de transferência eletrônica de fundos. A família de normas ISO 25000 define dois modelos-chave de qualidade: o modelo de qualidade do produto, que avalia o próprio software (ISO/IEC 25010, 2023), e o modelo de qualidade em uso, que avalia o efeito do software quando utilizado em um contexto específico (ISO/IEC 25019, 2023) . O foco aqui é o modelo de qualidade do produto, com a Tabela 2 ilustrando as nove características de qualidade e subcaracterísticas (ISO/IEC 25010).

Tabela 2. ISO/IEC 25010 Modelo de Qualidade do Produto

SOFTWARE PRODUCT QUALITY								
Functional Suitability	**Performance Efficiency**	**Compatibility**	**Interaction Capability**	**Reliability**	**Security**	**Maintainability**	**Flexibility**	**Safety**
Functional Completeness Functional Correctness Functional Appropriateness **Source: ISO2500.com**	Time Behavior Resource Utilization Capacity	Co-Existence Interoperability	Appropriateness Recognizability Learnability Operability User Error Protection User Engagement Inclusivity Self-Descriptiveness	Faultlessness Availability Fault Tolerance Recoverability	Confidentiality Integrity Non-repudiation Accountability Authenticity Resistance	Modularity Reusability Analyzability Modifiability Testability	Adaptability Scalability Installability Replaceability	Operational Constraint Risk Identification Fail Safe Hazard Warning Safe Integration

Embora todas as nove características sejam essenciais, manter a segurança e preservar a privacidade de informações pessoais e financeiras são fundamentais neste setor. Violações de dados podem ter impactos significativos, incluindo a exposição de informações de clientes a atacantes, danos à reputação da empresa, perdas financeiras substanciais e penalidades legais e processos judiciais. Dependendo do país, uma organização pode ser obrigada a arcar com os custos de monitoramento de crédito devido ao aumento de tentativas de phishing e golpes contra indivíduos.

A segurança cibernética é explorada em detalhes nos syllabi do ISTQB® Security Tester [ISTQB_CT-SEC_SYL] e do ISTQB® Security Test Engineer [ISTQB_CT-STE_SYL].

3.2 Princípios de Testes Baseados em Riscos em Sistemas Financeiros

Os testes baseados em riscos priorizam as atividades de teste com base no nível de risco. Em sistemas financeiros, onde o custo dos defeitos pode ser extremamente alto (p. ex., perdas financeiras, penalidades regulatórias, danos à reputação), os testes baseados em riscos são especialmente críticos. Embora as instituições financeiras tenham estruturas diferentes, elas compartilham funções semelhantes. É necessário analisar os processos de negócios, as transações financeiras, os requisitos de conformidade e as vulnerabilidades de segurança. As equipes buscam priorizar seus testes com base no risco. Além de calcular juros sobre depósitos e hipotecas, as instituições financeiras desempenham muitas outras funções, incluindo privacidade e segurança.

As equipes aplicam testes baseados em riscos priorizando áreas que apresentam o maior risco de conformidade ou de negócios. Uma vez identificado, cada risco é avaliado quanto à probabilidade de risco e ao impacto do risco . Um valor de nível de risco, chamado nível de risco, pode ser calculado (p. ex., probabilidade de risco * impacto do risco) para priorizar as áreas de foco dos testes. Os níveis de risco podem ser expressos quantitativamente (p. ex., 20% de chance de atraso) ou qualitativamente (p. ex., como baixo, médio ou alto).

Uma matriz de risco (também chamada de matriz de probabilidade-impacto) é uma ferramenta visual de gerenciamento de risco que mapeia os riscos identificados em uma grade, usando a probabilidade de risco (probabilidade de ocorrência) em um eixo e o impacto do risco (consequências caso ocorram) no outro. Os riscos com maior probabilidade e maior impacto recebem a prioridade máxima nos testes. Na avaliação dinâmica de riscos, os níveis de risco em sistemas financeiros evoluem à medida que novos recursos, integrações ou regulamentações são introduzidos. A reavaliação periódica de riscos verifica se as prioridades de teste permanecem alinhadas com as realidades comerciais e regulatórias atuais.

As razões para os testes baseados em riscos incluem:

- **Alocação eficiente de recursos** – as equipes podem planejar e alocar recursos para áreas com maior probabilidade de risco e maior impacto do risco,
- **Detecção precoce de defeitos** – permite que as equipes identifiquem defeitos críticos no início do SDLC (shift left), oferecendo a oportunidade de corrigir defeitos em código crítico durante o sprint/iteração atual,
- **Cobertura otimizada** – os testes podem ser concentrados em funcionalidades críticas e áreas de alta prioridade, para garantir que os aspectos mais importantes do software sejam testados exaustivamente,
- **Valor aprimorado de negócio**– ajuda a entregar software que atenda tanto aos requisitos de negócio quanto às expectativas dos clientes, contribuindo para aumentar a satisfação do cliente e a receita.

3.3 Atividades de Teste Relacionadas a Testes Baseados em Riscos

Tanto os riscos funcionais (p. ex., cálculos de juros incorretos) quanto os riscos não funcionais (p. ex., baixa performance sob alta carga) precisam ser considerados. Para identificar e priorizar os riscos, stakeholders como analistas de negócios, responsáveis pela conformidade, equipe técnica e gerentes de risco precisam estar envolvidas.

A identificação de quais riscos precisam de atenção imediata e quais podem ser monitorados ajuda as equipes a concentrar recursos de forma eficaz.

Priorize os esforços de teste. Existem várias técnicas para priorizar riscos, incluindo:

- Failure Mode and Effect Analysis (FMEA) – uma abordagem sistemática e proativa usada para identificar, priorizar e mitigar falhas potenciais em um projeto, processo ou serviço antes que elas ocorram.
- Fault Tree Analysis (FTA) – uma técnica de análise de falhas dedutiva e de cima para baixo, usada para identificar as causas-raiz de um evento indesejado no nível do sistema, mapeando graficamente as falhas de componentes por meio de portas lógicas booleanas (AND, OR).
- PRISMA (Product RISk MAnagement) – uma abordagem para identificar as áreas mais importantes a serem testadas, ou seja, identificar as áreas que apresentam o maior nível de risco comercial ou técnico (Veenendaal, 2012).

Definir as condições de teste . Crie condições de teste que abranjam as áreas de alto risco identificadas para verificar se a cobertura está alinhada com os níveis de risco e aborda riscos específicos, proporcionando uma cobertura abrangente e a mitigação dos riscos identificados. Para ajudar a determinar essa integridade e conformidade, podem ser criadas matrizes de rastreabilidade, vinculando os riscos às condições de teste e as condições de teste aos resultados dos testes.

Executar e monitorar os testes. Execute as suítes de testes criadas a partir dos casos de teste, com base nas condições de teste, monitorando de perto os resultados dos testes e coletando dados relevantes.

Relatar e mitigar riscos . Documentar e relatar quaisquer defeitos descobertos durante os testes. Estratégias de mitigação de riscos identificam, abordam, reduzem ou gerenciam riscos identificados que poderiam impactar negativamente um projeto, negócio ou operação. Estratégias padrão de mitigação de riscos são:

- prevenção de riscos – tomar medidas deliberadas para eliminar um risco específico, evitando o envolvimento em atividades que possam causá-lo,
- mitigação de risco por meio de testes – reduzir a probabilidade de risco ou o impacto do risco por meio de atividades de teste,
- transferência de risco – transferir o risco para um terceiro, como um seguro,
- aceite do risco – reconhecer e aceitar o risco.

A norma ISO 31000 « » (2018) fornece orientações adicionais sobre a integração do gerenciamento de risco nas atividades centrais e na tomada de decisões da organização. Essas orientações são: integradas, estruturadas e abrangentes, personalizadas, inclusivas e dinâmicas; utilizam as melhores informações disponíveis; levam em consideração fatores humanos e culturais; e promovem a melhoria contínua.

4 Teste e Gerenciamento de Dados de Teste – 90 minutos

Palavras-chave

precisão dos dados, consistência dos dados, reconciliação de dados, dados de teste, técnica de teste

Palavras-chave específicas do domínio

trilha de auditoria, sistema bancário central, confiança do cliente, privacidade do dado, perfil de dados, razão geral, sistema de liquidação

Objetivos de aprendizagem do Capítulo 4:

4.1 Precisão dos dados e consistência dos dados

FT-4.1.1 (K2) Explicar a importância da precisão e consistência dos dados em todos os sistemas financeiros

4.2 Reconciliação de dados entre sistemas financeiros

FT-4.2.1 (K3) Aplicar técnicas de reconciliação de dados a processos financeiros multissistemas

4.3 Privacidade do dado e proteção de dados em testes financeiros

FT-4.3.1 (K2) Explicar a importância da privacidade do dado e da proteção de dados em testes financeiros.

Introdução a Testes de Dados e Gerenciamento de Dados

No setor financeiro, a consistência dos dados, a precisão e a integridade dos dados são essenciais para a tomada de decisões acertadas e o cumprimento das regulamentações. Os testes de dados verificam a precisão, a integridade, a atualidade e a proveniência dos dados financeiros ao longo de todo o seu ciclo de vida, garantindo a conformidade com os frameworks de governança de dados. As instituições financeiras processam volumes massivos de dados transacionais e analíticos; portanto, os testes são necessários para verificar a precisão e a confiabilidade dos pipelines de dados, relatórios e modelos financeiros. Esta seção aborda as dimensões da qualidade dos dados, regras de validação e tipos de testes, como reconciliação, integridade, lógica de transformação e testes de regressão. O foco é o ciclo de vida dos dados financeiros, começando pela criação dos dados, passando pela geração de relatórios e identificando anomalias nos dados que possam afetar os níveis de risco, a conformidade ou a experiência do cliente.

4.1 Precisão e Consistência dos Dados

A **precisão dos dados** refere-se à forma correta como os dados representam informações financeiras reais. Dados precisos refletem o valor real das transações, saldos e detalhes dos clientes. São completos, atuais e livres de defeitos que poderiam distorcer o comportamento ou os resultados do sistema.

A **consistência dos dados** refere-se à representação uniforme dos dados em todos os sistemas, componentes e bancos de dados. Dados consistentes aparecem no mesmo formato, valor e significado onde quer que sejam usados, garantindo que os sistemas não apresentem informações conflitantes.

Importância nos sistemas financeiros

- Relatórios financeiros. Pequenas imprecisões ou inconsistências podem resultar em cálculos defeituosos, resumos enganosos e insights financeiros não confiáveis.
- Risco e apoio à decisão. Avaliações de risco e modelos analíticos dependem de grandes volumes de dados históricos e transacionais. Entradas inconsistentes ou com defeitos podem enfraquecer previsões, distorcer perfis de risco e reduzir a confiança nos resultados analíticos.
- Integração e automação de sistemas. As plataformas financeiras geralmente compreendem vários componentes interconectados, incluindo processamento de transações, gestão de clientes e sistemas de reconciliação. Dados consistentes permitem um fluxo de informações contínuo entre interfaces, camadas de integração e processos de transformação, reduzindo a intervenção manual e o atrito operacional.

Os defeitos típicos de precisão dos dados e de consistência dos dados incluem o seguinte:

- transações duplicadas que aparecem em extratos,
- diferenças de saldo entre sistemas de contabilidade geral e auxiliar,
- variações nos dados de clientes entre sistemas de integração e de identidade,
- incompatibilidades cambiais no processamento de transações internacionais,
- perda ou corrupção de dados durante atividades de migração ou transformação.

Áreas de foco dos testes. As atividades de teste concentram-se em determinar a precisão e a consistência dos dados à medida que estes são movidos, transformados e armazenados entre sistemas. Isso envolve comparar conjuntos de dados de origem e de destino, validar resultados de reconciliação de dados, confirmar a lógica das regras de negócios e avaliar o impacto das alterações no sistema sobre os

fluxos de dados existentes. Compreender as definições de dados mestres e de referência é essencial para manter uma interpretação consistente dos dados entre as aplicações.

Abaixo estão algumas práticas recomendadas a serem seguidas para ajudar a garantir a precisão dos dados e a consistência dos dados:

- aplicar as regras de validação de dados bem definidas e tratamento de exceções,
- utilizar técnicas de comparação automatizadas para grandes conjuntos de dados,
- realizar a análise de perfis de dados para avaliar estrutura, integridade e qualidade,
- identificar padrões incomuns ou anomalias em um estágio inicial,
- manter documentação clara para definições de dados e metadados.

4.2 Reconciliação de Dados entre Sistemas Financeiros

A reconciliação de dados trata do alinhamento dos dados financeiros à medida que estes transitam por múltiplos sistemas dentro de um ecossistema financeiro. As transações financeiras normalmente passam por várias plataformas, incluindo sistemas de processamento de transações, mecanismos de liquidação, plataformas contábeis e camadas de relatórios. As atividades de reconciliação garantem a confiança de que cada sistema reflete o mesmo resultado financeiro, apesar das diferenças na lógica de processamento, no tempo ou nas transformações de dados.

Essa área é particularmente relevante durante mudanças no sistema, incluindo migrações de sistemas bancários centrais, atualizações de plataforma e transferências de dados em grande escala. Mesmo quando os sistemas funcionam corretamente em nível técnico, lacunas na reconciliação podem levar a saldos incorretos, transações ausentes ou relatórios inconsistentes se os dados não estiverem alinhados entre os sistemas.

Contexto de migração e reconciliação de dados. Durante iniciativas de migração de dados , as instituições financeiras transferem grandes volumes de dados históricos e ativos, incluindo contas, saldos, transações e registros de clientes. A reconciliação, nesse contexto, concentra-se em confirmar que os dados extraídos de sistemas legados estejam total e corretamente representados no ambiente de destino após a transformação e o carregamento.

As técnicas de validação geralmente incluem amostragem de registros , comparações de agregação , verificação de checksum e correspondência de saldos entre os sistemas de origem e de destino. A reconciliação pós-migração compara indicadores financeiros-chave, como saldos iniciais, totais de transações e status de lançamento, para identificar discrepâncias introduzidas durante a migração ou transformação.

Reconciliação em ambientes financeiros integrados. Em ambientes operacionais , a reconciliação garante a consistência entre sistemas interconectados, como plataformas bancárias centrais, gateways de pagamento, sistemas de compensação e liquidação e data warehouses. O escopo vai além de registros individuais, abrangendo fluxos de trabalho comerciais completos. Por exemplo, espera-se que uma transação iniciada em um canal de atendimento ao público siga um ciclo de vida consistente — incluindo autorização, liquidação, estorno ou rejeição — em todos os sistemas a jusante.

A reconciliação eficaz também apoia relatórios financeiros e operacionais com alta confiabilidade, verificando se os valores agregados estão alinhados com os dados subjacentes no nível da transação.

Principais áreas de reconciliação

- **Alinhamento de dados entre sistemas**. A reconciliação examina como as transações são refletidas à medida que se movem entre sistemas, como de plataformas de processamento de

transações para sistemas de contabilidade e liquidação. Espera-se que os estados das transações, valores e carimbos de data/hora permaneçam alinhados entre as interfaces.

- **Definição do escopo da reconciliação**. A identificação clara de pontos de reconciliação, como saldos, contagem de transações, datas de lançamento e status, verifica a cobertura de processos financeiros críticos, incluindo depósitos, saques, transferências e pagamentos de empréstimos.
- **Níveis de tolerância e exceções**. Certas variações, como diferenças de arredondamento causadas pela conversão de moeda, podem estar dentro de limites de tolerância predefinidos. A reconciliação distingue variações aceitáveis de discrepâncias genuínas, com exceções identificadas para análise posterior.
- **Processamento em lote e tratamento de fechamento**. Muitos sistemas financeiros dependem de ciclos de processamento em lote programados, particularmente durante o processamento de fim de dia ou fim de período. A reconciliação considera o tratamento de transações em torno dos horários de fechamento (como o fim do mês) para verificar a integridade e evitar duplicações.
- **Reconciliação de livros contábeis e saldos**. Os dados no nível da transação são alinhados com os lançamentos nos livros auxiliares e no razão geral. As diferenças, incluindo saldos em suspenso ou não correspondentes, são rastreadas até serem resolvidas.
- **Frequência da reconciliação e tratamento de volume**. A reconciliação pode ser realizada em tempo real, intra-dia ou no final do dia, dependendo das necessidades do negócio. O comportamento do sistema sob picos de volume de transações é observado para verificar se os processos de reconciliação permanecem estáveis e com alta confiabilidade.
- **Transformação de dados e validação de mapeamento**. Os dados financeiros frequentemente passam por transformações, como aplicação de taxas, cálculo de juros e conversão de moeda. A reconciliação confirma que as regras de transformação produzem resultados consistentes entre os sistemas.
- **Transações multimoeda e transfronteiriças**. As transações internacionais introduzem uma complexidade adicional na reconciliação devido às taxas de câmbio, moedas de liquidação e diferenças de prazo. O alinhamento entre os valores convertidos e os valores de liquidação é um ponto-chave.

Exemplos de cenários de reconciliação específicos para transações incluem:

- **Transações com cartão**. Os pagamentos com cartão envolvem sistemas emissores, plataformas de aquisição, redes e mecanismos de liquidação. A reconciliação concentra-se em valores de transação, taxas, estornos, cobranças reversas e lançamentos de liquidação.
- **Transações em caixas eletrônicos.** A atividade em caixas eletrônicos abrange switches, processadores e sistemas bancários centrais. A reconciliação abrange saques em dinheiro, taxas, estornos, saques parciais e cenários de exceção

4.3 Privacidade de Dados e Proteção de Dados em Testes Financeiros

Os sistemas financeiros processam informações altamente confidenciais, incluindo dados pessoais, detalhes de transações e informações institucionais. Durante os testes, tais dados devem ser protegidos contra acesso não autorizado, divulgação, alteração ou uso indevido. Os testes também devem confirmar que o sistema lida com os dados de acordo com os requisitos de privacidade e proteção aplicáveis.

A privacidade do dado diz respeito à coleta, uso, armazenamento, compartilhamento e exclusão adequados de informações pessoais e financeiras, em conformidade com os requisitos legais, regulatórios e organizacionais.

Exemplos de áreas relacionadas à privacidade a serem testadas incluem:

- acesso a dados confidenciais de acordo com as funções e responsabilidades dos usuários
- restrição da visibilidade de dados confidenciais em telas, relatórios, exportações e mensagens de erro.
- uso de dados pessoais apenas para fins autorizados e de acordo com o consentimento.
- implementação correta das regras de retenção e exclusão de dados.
- compartilhamento controlado de dados por meio de interfaces e sistemas externos.
- registro de acessos e ações em dados confidenciais para garantir a contabilização e a auditabilidade.

Os riscos típicos de privacidade em testes financeiros incluem a exposição não intencional de dados pessoais ou financeiros, o vazamento de dados confidenciais por meio de registros ou relatórios, a aplicação inconsistente de controles de privacidade e o comportamento do sistema não alinhado aos requisitos de privacidade.

A proteção de dados diz respeito à salvaguarda de informações confidenciais, especialmente em ambientes de teste. Dados reais de produção devem ser evitados, a menos que sejam fortemente mascarados ou anonimizados sob controles rigorosos. Sempre que possível, dados sintéticos, anonimizados, pseudonimizados ou mascarados devem ser usados para testes.

Exemplos de áreas relacionadas à proteção de dados a serem testadas incluem:

- classificação de dados de acordo com a sensibilidade, para que controles apropriados possam ser aplicados
- mascaramento ou anonimização de valores confidenciais, preservando a usabilidade do teste
- substituição de identificadores por meio de pseudonimização para reduzir a exposição de dados pessoais
- restrição do acesso apenas a pessoal autorizado
- retenção de dados de teste apenas pelo período necessário, seguida de remoção segura de dados
- proteção de logs e resultados de monitoramento para que dados confidenciais não sejam exibidos em texto simples

O teste de privacidade e proteção de dados em sistemas financeiros ajuda a reduzir riscos de conformidade, segurança e operacionais, ao mesmo tempo em que apoia o tratamento confiável de informações confidenciais.

5 Teste Funcional e Teste Não Funcional – 165 minutos

Palavras-chave

disponibilidade, testes back-to-back, testes de cálculo, testes exploratórios, testes funcionais, testes de carga, testes não funcionais, testes de performance, testes de segurança, testes de estresse

Palavras-chave específicas do domínio

GenAI

Objetivos de aprendizagem do Capítulo 5:

5.1 Teste funcional de sistemas financeiros

FT-5.1.1 (K3) Aplicar testes funcionais para validar sistemas financeiros

5.2 Riscos de performance em finanças

FT-5.2.1 (K2) Explicar os riscos de performance em sistemas financeiros durante períodos de pico

5.3 Teste de performance em contextos financeiros

FT-5.3.1 (K3) Aplicar testes de carga e testes de estresse em contextos específicos da área financeira

5.4 Teste de segurança e teste de disponibilidade

FT-5.4.1 (K2) Explicar as necessidades de testes de segurança e de disponibilidade em sistemas financeiros

5.5 GenAI em testes financeiros

FT-5.5.1 (K2) Explicar como a GenAI pode apoiar e melhorar os testes financeiros

Introdução ao Teste Funcional e ao Teste Não Funcional

Os testes de software financeiro são cruciais para garantir a segurança, a funcionalidade, a confiabilidade e a conformidade das aplicações financeiras. Normalmente, envolvem vários tipos de testes, incluindo testes funcionais, de segurança, de performance e de conformidade, para proteger contra riscos e aumentar a confiabilidade do software.

5.1 Teste Funcional de Sistemas Financeiros

Como os sistemas financeiros lidam com dados financeiros confidenciais e transações monetárias reais, o custo de uma falha é muito alto. Os testes exigem uma abordagem abrangente, em conformidade e baseada em riscos, cobrindo fluxos críticos de negócios, o que requer sólido conhecimento da área e consciência das regulamentações e riscos.

No setor financeiro, os testes funcionais (especialmente as técnicas de teste caixa-preta) desempenham um papel fundamental no apoio à correção funcional e no cumprimento dos requisitos funcionais. Isso inclui:

- verificar funções financeiras essenciais, como gestão de contas, processamento de transações e relatórios,
- definir o escopo dos objetivos funcionais e a estratégia de cobertura,
- realizar priorização baseada em riscos,
- determinar a conformidade com regulamentações, como o GDPR ou o PCI DSS (ver Capítulo 2).

Várias técnicas de teste são particularmente relevantes para validar os principais recursos financeiros (ver [ISTQB_CTFL_SYL], Seção 4.2):

- particionamento de equivalência – verificação da correção funcional e da consistência das transações,
- análise de valor limite – verificação dos valores limites com precisão monetária (p. ex., incrementos de 0,01), incluindo arredondamento na menor unidade e valores limítrofes (imediatamente abaixo, no limite ou imediatamente acima),
- teste de tabela de decisão – validação dos resultados do teste para combinações de regras e condições de negócios, uma vez que o teste de tabela de decisão é utilizado para testar combinações,
- teste de transição de estado – testar estados de conta, como ativo/inativo/bloqueado.

A Tabela 3 fornece exemplos de técnicas de teste funcional adicionais adequadas para sistemas de software financeiro.

Tabela 3. Exemplos de técnicas de teste utilizadas em testes financeiros

Técnica de teste / abordagem de teste		Vantagens, desvantagens e desafios
Testes de cálculo	Essa técnica de teste envolve o recálculo de valores utilizando funções e fórmulas conhecidas. Isso é necessário ao definir fórmulas corretas e valores limite. Alguns exemplos incluem o cálculo de fluxos de caixa,	**Vantagens:** resultados do teste com alta confiabilidade, facilmente formalizáveis e documentáveis. **Desvantagens:** aplicabilidade limitada para testes analíticos

Técnica de teste / abordagem de teste		Vantagens, desvantagens e desafios
	o valor presente líquido de fluxos de caixa futuros e os preços de opções. A verificação por meio de testes de cálculo concentra-se na identificação de relações formais es entre variáveis, em vez de calcular diretamente os resultados.	complexos devido a extensos requisitos de documentação e implementação. **Desafios:** requer profundo conhecimento da área.
Teste exploratório	Esta abordagem de teste concentra-se na identificação de padrões comportamentais em valores financeiros sem exigir cálculos explícitos. Os casos de teste verificam relações de entrada-saída, validam suposições de variáveis, aplicam valores-limite (p. ex., exceder o limite do valor de transferência) e utilizam testes exploratórios para descobrir defeitos de cálculo,	**Vantagens:** execução rápida, ampla cobertura, baixo custo. **Desvantagens:** impossibilidade de integração em frameworks de automação ou pipelines de CI/CD. **Desafios:** requer qualificações sólidas e conhecimento específico da área.
Teste back-to-back		**Vantagens:** eficaz para testes de regressão. **Desvantagens:** a configuração de ambientes de teste e a sincronização de parâmetros de entrada podem ser difíceis, especialmente ao manter várias versões de aplicativos. **Desafios:** a análise de discrepâncias exige profundo conhecimento da área e familiaridade com ambos os sistemas.

Com base no tempo, nas necessidades de cobertura e nas habilidades da equipe, escolher o conjunto certo de técnicas de teste é fundamental para obter resultados de teste eficientes e completos. Por exemplo, os testes de caixas eletrônicos incluem técnicas básicas (análise de valor limite para transferências mínimas/máximas) e especializadas: testes back-to-back, testes de correção funcional de cálculos de taxas e moedas e testes exploratórios para novos modelos de caixas eletrônicos.

Para maximizar a efetividade dos testes funcionais, considere adotar as seguintes práticas recomendadas:

- colete feedback real dos usuários,
- utilize dispositivos reais – emuladores e simuladores não podem ser uma solução de longo prazo para testes de dispositivos,
- teste com dados semelhantes aos de produção (p. ex., dados reais anônimos ou dados de testes sintéticos realistas),
- coordenar e alinhar os esforços de teste entre especialistas de negócios e testadores para alcançar um entendimento comum e uma responsabilidade conjunta.

5.2 Riscos de Performance no Setor Financeiro

As instituições financeiras dependem de sistemas de software confiáveis para processar grandes volumes de transações financeiras, dar suporte a serviços de pagamento, gerenciar investimentos e cumprir requisitos regulatórios. Esses sistemas devem manter uma eficiência de performance aceitável sob condições operacionais variáveis, particularmente durante períodos de pico de transações, ao mesmo tempo em que preservam a integridade dos dados. Os riscos de performance referem-se à possibilidade de tempos de resposta inaceitáveis, atrasos no processamento ou degradação da taxa de processamento quando os volumes de transações ou a carga do sistema excedem os níveis operacionais normais.

Os desafios comuns de performance em instituições financeiras incluem:

- Escalabilidade – sistemas incapazes de escalar efetivamente com o aumento da carga de usuários. Por exemplo, um sistema de processamento de pagamentos apresenta falhas de performance durante horários de pico (feriados, Natal, Black Friday, quedas no mercado).
- Defeitos de concorrência – incapacidade de gerenciar solicitações simultâneas. Por exemplo, após falhas em massa, os funcionários da plataforma de negociação começam a recarregar a página do aplicativo para reiniciar o serviço.
- Limitações de infraestrutura – hardware desatualizado ou configurações ineficientes que impedem a performance ideal. Por exemplo, sistemas de gestão de investimentos estão enfrentando falhas de performance, mas não conseguem migrar rapidamente para soluções externas baseadas em nuvem.
- Violações de integridade de dados – perda ou corrupção de dados transacionais sob carga pesada. Por exemplo, quando um banco prepara relatórios anuais para reguladores, pode enfrentar falhas de performance que levam à perda de dados e a sanções regulatórias.
- Riscos de dívida técnica – a necessidade de atualizar tanto o software quanto os componentes de hardware desatualizados, que podem falhar prematuramente, aumentar significativamente os custos de manutenção e levar à indisponibilidade de sistemas financeiros altamente carregados.
- Dependências de terceiros – dependência de fornecedores externos de software, serviços em nuvem e provedores de gateways de pagamento, cuja indisponibilidade pode afetar as operações de performance internas.

Ignorar os riscos de performance de software expõe as instituições financeiras a perdas financeiras e danos à reputação de severa gravidade (p. ex., reclamações públicas de clientes nas redes sociais causando perda de confiança). As atividades para minimizar esses problemas incluem:

- monitoramento contínuo,
- programas de treinamento de funcionários,
- auditorias regulares,
- as atividades de teste estático incluem a análise de métricas de carga do sistema e a comparação dessas métricas com uma linha de base acordada com analistas de negócios, para determinar se são necessárias alterações no perfil de carga,
- processos de teste focados na confiabilidade, incluindo testes de performance e de disponibilidade programados regularmente.

5.3 Teste de Performance em Contextos Financeiros

Os testes de performance (p. ex., teste de estresse, teste de carga) desempenham um papel importante na avaliação da confiabilidade e resiliência dos sistemas financeiros e devem ser obrigatórios em ambientes regulamentados. A estratégia de teste pode especificar um ambiente separado e dedicado para testes de carga que reflita fielmente as características do ambiente de produção. Isso requer forte isolamento e um alto grau de semelhança com a produção, incluindo configurações alinhadas, procedimentos de sincronização, gerenciamento de dependências e versões consistentes de serviços externos. Ele se aplica aos dados, sua estrutura e quantidade. Os testes de performance são frequentemente realizados diariamente. Alternativamente, as equipes podem usar monitoramento contínuo de performance ou testes de performance noturnos. Mais informações sobre conceitos gerais em testes de performance podem ser encontradas em [ISTQB_CT-PT_SYL].

Exemplos de eventos que exigem testes de performance em sistemas financeiros incluem:

- implantação inicial em produção ou um lançamento importante (p. ex., adicionar integração com um serviço de monitoramento de fraudes a um aplicativo bancário),
- mudanças significativas no sistema, como atualizações de software (p. ex., migração para uma nova versão principal do banco de dados) ou mudanças arquitetônicas (p. ex., mudança de uma arquitetura monolítica para microsserviços),
- mudanças esperadas no perfil de carga (p. ex., a abertura de novos escritórios levando a um aumento na base de clientes de uma empresa de corretagem).

Para sistemas financeiros de alta carga, as tarefas típicas de testes de performance podem incluir as seguintes etapas:

- iniciar,
- reunir e analisar métricas históricas de picos de volume,
- preparar o plano de teste de performance e definir métricas aceitáveis (SLAs),
- preparar o ambiente de teste, os dados de teste e as ferramentas de teste de performance,
- executar os testes de performance,
- analisar os resultados dos testes e preparar o relatório de testes de performance.

As tarefas de teste de performance são abordadas em detalhes em [ISTQB_CT-PT_SYL], Capítulo 4.

Os sistemas financeiros frequentemente enfrentam picos de volume de transações (p. ex., prazos fiscais, picos de vendas no varejo, sessões de negociação). Para abordar os riscos de desempenho descritos na Seção 5.2, a Tabela 4 fornece exemplos de testes de performance adicionais aplicáveis a sistemas de software financeiro.

Tabela 4. Atividades adicionais que apoiam o teste de sistemas de software financeiro"

Atividades	Descrição
Teste de carga	Valida a funcionalidade do sistema sob níveis de carga especificados usando métricas, como transações por segundo.
Teste de estresse	Verifica o comportamento do sistema sob cargas que excedem as condições normais ou de pico esperadas (p. ex., até 200%). Resultado esperado: o sistema pode apresentar desempenho reduzido ou falhas parciais, mas deve falhar de forma controlada (p. ex., retornar erros significativos, sem travar

Atividades	Descrição
	completamente) e se recuperar para níveis de performance aceitáveis assim que a carga voltar ao normal. Métricas: latência de solicitação, taxa de erros, taxa de transferência e utilização de recursos (CPU, memória) durante e após o período de estresse.
Resistência	Determine se o SUT opera de forma estável sob carga sustentada ao longo do tempo. Métricas de monitoramento, como a unidade central de processamento (CPU) e a utilização de recursos, podem ajudar a detectar degradação (p. ex., vazamentos de memória). Isso se aplica ao teste de resistência.
Disponibilidade do sistema externo	Mede o desempenho e a estabilidade do sistema (tempos de resposta, taxas de erro, consumo de recursos) quando sistemas externos dependentes estão lentos, em tempo limite ou indisponíveis. Ajuda a garantir que a lógica de tratamento de falhas (disjuntores, tentativas de repetição) não introduza degradação de desempenho ou vazamentos de recursos. Métricas: uso de CPU/memória, percentis de latência de solicitação, número de exceções de tempo limite.
Failover	Verifica a estabilidade do sistema após reinicialização, resiliência a falhas, velocidade de recuperação e backup. Sistemas baseados em nuvem podem excluir pods durante os testes. Aplícável para testes de pico, que determinam a resiliência do sistema contra picos repentinos de carga e a recuperação para operação estável.
Disponibilidade do data center	Testa o balanceamento correto de solicitações entre data centers durante o tempo de inatividade, usando métricas como taxa de falha, transações e solicitações HTTP por segundo. Útil para testes de escalabilidade, teste de pico e teste de estresse .

Ao implementar procedimentos regulares de testes de performance e investir em infraestrutura de confiabilidade elevada, as instituições financeiras podem reduzir o risco de interrupções de serviço onerosas.

5.4 Teste de Segurança e Teste de Disponibilidade

Os testes de segurança de softwares financeiros verificam se o sistema protege a confidencialidade, a integridade e a disponibilidade dos dados, ajudando assim a prevenir fraudes e perdas financeiras. Essas atividades devem ser integradas ao longo de todo o ciclo de vida de desenvolvimento de software, por exemplo, identificando precocemente lacunas nas normas e aplicando modelagem de ameaças para mitigar riscos financeiros, ou realizando revisões de segurança especializadas em projetos e arquiteturas.

Os tipos de testes de segurança incluem:

- varredura de vulnerabilidades,
- testes de penetração,
- Static/Dynamic Application Security Testing (SAST/DAST),
- análise de dependências e componentes de terceiros.

As principais áreas de testes financeiros incluem:

- teste de configurações em nuvem e gerenciamento de segredos para conformidade (p. ex., para processamento de pagamentos),
- teste de algoritmos de criptografia de dados (p. ex., nos setores contábil e bancário),
- validação da autenticação multifatorial, controles de acesso baseados em funções, ciclos de vida de tokens e verificação de que há segurança no roteamento do tráfego de API por meio de gateways dedicados (p. ex., aplicativos móveis e de internet banking),
- verificação da integridade dos logs de segurança, configuração, procedimentos de gerenciamento e alertas (p. ex., proteção das informações pessoais dos segurados no setor de seguros).

Algumas das melhores práticas para a realização de testes de segurança incluem:

- uso de ferramentas especializadas,
- seguir as normas aplicáveis (p. ex., OWASP),
- integrar a segurança no processo de desenvolvimento (DevSecOps),
- incorporar modelagem de ameaças,
- gerenciar riscos relacionados a terceiros e à cadeia de suprimentos,
- projetar ambientes de teste seguros e lidar com os dados de teste de forma responsável,
- alinhamento com testes de conformidade (consulte o Capítulo 2).

Para mais informações, consulte [ISTQB_CT-SEC_SYL].

O **teste de disponibilidade** determina se há operação contínua durante picos de carga para evitar perdas de transações, impacto na receita e perda da confiança do cliente. Os principais objetivos e métricas relacionadas incluem:

- metas de recuperação: Recovery Time Objective (RTO) para serviços de TI e Recovery Point Objective (RPO) para transações-chave,
- performance sob carga: tempo de execução, tempo de resposta e taxa de transferência para transações-chave,
- confiabilidade do sistema: taxa de falha, Mean Time Between Failures (MTBF), Mean Time to Failure (MTTF) e disponibilidade,
- validação da resiliência: balanceamento de carga, testes de failover e Mean Time to Repair (MTTR).

As estratégias de teste para mitigar os desafios de disponibilidade incluem:

- escalabilidade: realizar testes de carga e de estresse utilizando cenários de horário de pico e validar o comportamento do escalonamento automatizado,
- infraestrutura: realizar testes sistemáticos de failover para verificar o comportamento de recuperação e a continuidade,

Teste de segurança e testes de disponibilidade são essenciais para sistemas de software financeiro confiáveis. Os testes de segurança protegem contra ataques maliciosos, enquanto os testes de disponibilidade verificam a continuidade do serviço e a recuperação em condições adversas. Juntas, essas atividades contribuem para a confiabilidade e resiliência geral do sistema.

5.5 GenAI em Testes de Software Financeiro

A integração da Inteligência Artificial Generativa (GenAI) nos testes de sistemas financeiros pode melhorar a eficiência e a consistência em um ambiente altamente regulamentado. Ao aplicar técnicas de engenharia de prompts, a GenAI pode apoiar as atividades de teste em todo o processo de teste, incluindo análise de teste, modelagem de teste, implementação de testes, monitoramento de teste e controle de teste, e conclusão do teste.

As organizações financeiras podem adotar os assistentes de IA comuns listados na Tabela 5 em seu SDLC.

Tabela 5. Assistentes de IA comuns aplicáveis em testes financeiros

Atividades de teste	Aspecto assistente da IA
Teste na fase de desenvolvimento	Assistentes de IA integrados podem ajudar os desenvolvedores a gerar testes de unidade e resolver automaticamente pequenos defeitos usando modelos adaptados aos padrões de codificação e padrões estabelecidos da organização.
Análise de teste	O assistente de IA auxilia os testadores ao analisar APIs e sugerir requisitos e condições de teste para revisão e aprimoramento.
Modelagem de teste e implementação de testes	O assistente de IA: - cria e sincroniza modelos de teste a partir do código, gera casos de teste em ambientes de desenvolvimento e envia os resultados dos testes para ferramentas de gerenciamento de teste, - cria e realiza revisões de testes automatizados com base em casos de teste existentes e gera casos de teste de interface do usuário e API a partir de requisitos, - verifica se os casos de teste violam os requisitos de segurança da informação, - permite a automação de testes com pouco ou nenhum código, ajudando os testadores a criar scripts de teste automatizados assistidos por IA usando interfaces visuais e componentes pré-construídos, reduzindo o esforço de codificação manual.
Monitoramento de teste e controle de teste	O assistente de IA analisa os registros de teste para detectar anomalias e identificar defeitos durante os testes.
Conclusão do teste	O assistente de IA oferece suporte à criação e validação de relatórios de teste e relatórios de defeitos.

A IA Gerativa pode aprimorar os testes de software financeiro, mas também traz desafios, especialmente a disponibilidade limitada e o alto custo de dados rotulados de alta qualidade. Para maximizar o valor da IA Gerativa, as instituições financeiras devem priorizar a integridade dos dados, o cumprimento das regulamentações, o desenvolvimento de competências e melhorias na infraestrutura. Os riscos econômicos devem ser gerenciados por meio de iniciativas-piloto e de um planejamento realista. O sucesso deve ser medido usando métricas claras (p. ex., tempo do ciclo de teste e taxas de defeitos) e avaliando oportunidades como geração autônoma de testes e monitoramento contínuo de conformidade. É provável que as funções de controle da qualidade se expandam para incluir mitigação proativa de risco, aprendizado contínuo, supervisão do treinamento de modelos de IA, adoção de melhores práticas e alinhamento com as metas de negócios. Habilidades avançadas em análise e depuração de IA se tornarão cada vez mais importantes.

6 Automação de Testes – 105 minutos

Palavras-chave

automação de testes

Palavras-chave específicas do domínio

DTO, privacidade

Objetivos de aprendizagem do Capítulo 6:

6.1 Papel da automação de testes nos testes financeiros

FT-6.1.1 (K2) Explicar como a automação de testes contribui para a eficiência dos testes na área financeira

6.2 Estratégias de automação de testes

FT-6.2.1 (K3) Aplicar estratégias de automação de testes em ambientes de TI financeiros legados e modernos

6.3 Desafios da automação de testes em ambientes regulamentados

FT-6.3.1 (K2) Explicar os desafios da automação de testes em ambientes regulamentados

6.4 Desafios em diferentes tipos de automação de testes

FT-6.4.1 (K2) Explicar os desafios da automação de testes em componentes móveis, front-end e back-end

Introdução à Automação de Testes

A automação de testes desempenha um papel importante na melhoria da estabilidade e da eficiência dos testes em sistemas financeiros. No setor financeiro, onde precisão e velocidade são essenciais (p. ex., no cálculo de juros compostos, na verificação de pontuações de crédito ou na execução de suítes extensivas de testes de regressão), a automação oferece vantagens significativas em relação aos testes manuais. Utilizando ferramentas e frameworks especializados, os engenheiros de testes podem validar com eficiência cálculos complexos, realizar simulações de altos volumes de transações e verificar a conformidade com os requisitos regulatórios. Para obter informações adicionais, consulte o [ISTQB_CTAL-TAE_SYL].

6.1 Papel da Automação de Testes nos Testes Financeiros

A automação de testes oferece benefícios significativos para o teste de sistemas financeiros, como ciclos de teste mais curtos, maior precisão e melhor escalabilidade. Exemplos incluem:

- A automação da execução de teste permite a execução consistente de testes e fornece resultados precisos, minimizando discrepâncias causadas por erros de entrada manual.
- A automação permite testes de regressão rápidos após atualizações (p. ex., funções de crédito ou pagamento), liberando os testadores manuais para se concentrarem em cenários complexos.
- Scripts de teste automatizados podem ser programados para execução frequente, alinhada com as implantações, fornecendo feedback rápido e apoiando a entrega iterativa.
- Os testes automatizados podem realizar a simulação de cenários de pico de carga e ser executados de forma consistente em vários ambientes com configurações alinhadas.
- Maior conformidade e segurança – a automação de testes pode verificar sistematicamente a conformidade com normas (p. ex., PCI DSS para pagamentos com cartão e controles AML/CFT) e gerar evidências auditáveis. Testes automatizados também podem ser executados em ambientes restritos sem conceder acesso manual, por meio da execução de scripts de teste repetíveis em pipelines controlados.
- Processos automatizados podem criar dados de teste complexos de ponta a ponta (p. ex., clientes com histórico de crédito, faturas, cartões e modelos de transação).

Apesar de suas vantagens, a implementação da automação de testes apresenta obstáculos únicos específicos do setor financeiro:

- **Complexidade** – os sistemas financeiros frequentemente envolvem fluxos de trabalho complexos que exigem algoritmos avançados para realizar uma simulação precisa de cenários do mundo real. Por exemplo, automatizar testes para um processo de registro de hipotecas pode exigir cobertura de pontuação, verificação de renda, cálculos de pagamento e integrações com registros externos.
- **Custo** – o esforço e as despesas iniciais para projetar, implementar e manter uma automação de testes eficaz podem ser significativos. Em sistemas financeiros, o retorno sobre o investimento é frequentemente impulsionado menos pela redução dos testes manuais e mais pela redução da probabilidade de risco e do impacto do risco de falhas de alto custo, como interrupções de serviço, transações que falham e penalidades regulatórias.
- **Lacuna de competências** – a falta de profissionais que compreendam tanto a lógica financeira dos negócios quanto as competências técnicas necessárias para a automação de testes pode limitar a adoção e a escalabilidade das iniciativas de automação de testes.

Para resolver essas questões, é necessário:

- planejamento estratégico,
- investimento em programas de treinamento (matrizes de competências, planos de desenvolvimento individual e mentoria),
- frameworks de teste e ferramentas de teste padronizadas (p. ex., para simular APIs externas)
- integração da automação de testes no ciclo de vida de desenvolvimento por meio de pipelines de CI/CD,
- colaboração entre as partes interessadas em todos os níveis de teste, e esses elementos devem ser refletidos na estratégia de automação de testes.

6.2 Estratégias de Automação de Testes

A automação de testes oferece vantagens significativas, incluindo economia de tempo e custos. No entanto, projetar e implementar uma estratégia de automação de testes ideal requer planejamento cuidadoso e consideração de vários fatores. Estratégias comuns de automação de testes incluem:

- Diferentes padrões de distribuição de testes (pirâmide, cone de sorvete, ampulheta, guarda-chuva) orientam os níveis de automação de testes, ajudando a avaliar os estados atuais e definir metas de melhoria. Sistemas legados exigem estratégias distintas em comparação com novas implementações.
- O "shift left" prioriza a automação precoce de testes e a conformidade nos fluxos de desenvolvimento, enquanto o "shift right" monitora a qualidade em tempo real, a integridade das transações e a detecção de fraudes em ambientes de produção.
- Em uma organização financeira com um cenário de infraestrutura complexo (p. ex., um sistema de processamento legado integrado a um aplicativo moderno de pagamento móvel), diferentes abordagens de teste são utilizadas dependendo do modelo de ciclo de vida de desenvolvimento de software, tais como:
  - práticas de desenvolvimento ágil de software, com ênfase na automação de testes,
  - modelos SDLC legados (p. ex., desenvolvimento de software sequencial), nos quais os testes são frequentemente planejados e executados em fases distintas,
  - práticas de DevOps, que permitem testes contínuos por meio de pipelines de CI/CD.

Por exemplo, ao dar preferência, inicialmente, à automação de testes em todas as camadas da pirâmide de testes — como testes de componentes, testes de API/serviços e testes de interface do usuário —, um banco pode liberar capacidade de teste para se concentrar na validação de dispositivos reais, como caixas eletrônicos e terminais de ponto de venda, que são caros e difíceis de automatizar. Neste exemplo, o banco implementa um conjunto de abordagens de teste: utiliza um esquema de distribuição de testes, concentra-se na automação de testes e dá prioridade à automação precoce de testes.

Para obter informações adicionais sobre abordagens de teste comuns ao definir uma estratégia de automação de testes, consulte o [ISTQB_CT-TAS_SYL], seção 3.1.1.

Além das abordagens comuns, é necessário observar as especificidades inerentes ao setor financeiro. Ao planejar uma estratégia de automação de testes para o setor financeiro, é importante considerar os seguintes fatores que podem influenciar as decisões:

- Exigências de alta precisão – defeitos em cálculos financeiros podem ter consequências graves. Por exemplo, os sistemas financeiros podem armazenar valores monetários usando diferentes tipos de dados e realizar cálculos com níveis variáveis de precisão. Ao definir a estratégia de

teste, é importante levar em conta essas diferenças e verificar se os testes aplicam precisão e verificação mais rigorosas do que normalmente seria exigido em domínios não financeiros.

- A implementação de testes automatizados de ponta-a-ponta em vários sistemas financeiros interconectados introduz uma complexidade técnica significativa, particularmente em áreas como sistemas contábeis com fluxos de trabalho de faturamento complexos.
- Uso de dados em tempo real (ou o mais próximo possível) em scripts de teste automatizados – a estrutura e o conteúdo dos dados de entrada podem mudar com o tempo. Por exemplo, os padrões de transações dos clientes podem variar de acordo com a estação do ano e com as ofertas de produtos. Os testes automatizados devem refletir cenários do mundo real da forma mais fiel possível, utilizando dados de pré-produção em estado de anonimização ou dados de teste atualizados regularmente.
- Oráculo de teste automatizado (ou pseudo-oráculo) – ao desenvolver um novo sistema, os resultados dos testes podem ser comparados com um aplicativo de referência. Essa abordagem pode ser limitada, pois manter os dois sistemas alinhados é um desafio, e diferenças nas regras de negócios ou no processamento de dados podem afetar os resultados dos testes.
- Abordagem para testes de regressão automatizados – compare os cálculos da aplicação atual com versões anteriores ou resultados de testes de referência para verificar a correção, levando em conta os custos de manutenção de ambientes de teste duplos.

6.3 Desafios da automação de testes em ambientes regulamentados

Organizações que atuam no setor financeiro devem cumprir vários conjuntos de regras, tanto nacionais quanto internacionais, como GDPR, SOX, PCI DSS e DORA. Essas regras impõem desafios adicionais que precisam ser considerados ao planejar uma estratégia de automação de testes:

- **Complexidade das regulamentações** – as regulamentações introduzem complexidade ao impor requisitos rigorosos de proteção de dados, privacidade e segurança, impactando os projetos de automação de testes. Um exemplo é a adesão aos padrões PCI DSS ao testar transações em caixas eletrônicos.
- **Problemas de manutenção** – a manutenção da automação de testes envolve tarefas regulares, como modificar o código da aplicação, gerenciar scripts de teste e bibliotecas de teste, atualizar integrações externas e ajustar suítes de teste.
- **Registro e comprovação** – os registros de transações comerciais devem ser mantidos e conservados, juntamente com os registros de teste, para validação pelos auditores. Os órgãos reguladores exigem comprovação da eficácia dos testes e da reprodutibilidade dos caminhos das transações para investigações.
- **Ferramentas específicas de teste automatizado** – as organizações financeiras frequentemente dependem de ferramentas proprietárias de automação de testes adaptadas às suas necessidades específicas. Essas ferramentas carecem de ampla representação no mercado e de suporte centralizado, por exemplo, ferramentas de teste para testes biométricos e PDVs/caixas eletrônicos.

As atividades para superar os desafios incluem:

- Complexidade das regulamentações
  - Criação de um mapa de testes para a complexidade das regulamentações, ou seja, uma tabela na qual a área de impacto, os requisitos de dados de teste e as condições de teste críticas são definidos para cada requisito regulatório.

- Anonimização de dados (mascaramento). Modificar dados reais removendo ou ofuscando identificadores pessoais, de modo que os dados permaneçam estruturalmente intactos e realistas para testes, mas não sejam mais considerados dados pessoais sob regulamentações como o GDPR.
- Geração de dados de testes sintéticos. Criar conjuntos de dados artificiais que imitem características do mundo real, garantindo que estejam livres de quaisquer restrições regulatórias.

- Problemas de manutenção
  - Use um objeto de transferência de dados (DTO) comum, se tal for definido pelo contrato de interação.
  - Dentro do framework de automação de testes, o isolamento da lógica de teste dos recursos (detalhes da interface do usuário, dados de teste) deve ser implementado.
  - Implemente a execução automática de scripts de teste automatizados a cada alteração de código para identificar rapidamente defeitos.
- Registro e comprobabilidade
  - Implemente o registro de testes de ponta-a-ponta. Cada rodada de teste deve gerar automaticamente um relatório de testware detalhado e estruturado.
  - Automatize a geração de relatórios de auditoria. Desenvolva relatórios automatizados que demonstrem a cobertura de funções críticas para conformidade, seu histórico de execução e comprovação de execução antes do lançamento.
- Ferramentas específicas de teste automatizado
  - Colocar o código-fonte de ferramentas internas em repositórios internos compartilhados com acessibilidade em toda a organização (inner source).
  - Ao desenvolver ferramentas internas, é necessário considerar a possibilidade de integrá-las por meio de protocolos padrão (REST API).

6.4 Desafios em Diferentes Tipos de Automação de Testes

À medida que a complexidade dos sistemas financeiros aumenta devido aos avanços em tecnologias como computação em nuvem, arquiteturas orientadas a serviços, IA e plataformas móveis, as abordagens de teste manual enfrentam inúmeros desafios. De aplicativos de serviços bancários móveis a sistemas financeiros em nuvem, essas aplicações exigem testes rigorosos para determinar a confiabilidade, a segurança e a conformidade regulatória. A automação de testes pode otimizar esse processo, mas também apresenta desafios, particularmente nos testes de componentes móveis, front-end e back-end.

Embora a automação de testes traga vantagens consideráveis, certos desafios persistem:

- **Automação de aplicativos móveis** – no setor financeiro, é importante considerar questões de segurança e conformidade, usabilidade e experiência do usuário, incluindo variação nas condições de rede, otimização da duração da bateria, fragmentação de dispositivos e desafios específicos de conformidade relacionados à segurança ou encriptação.
- **Automação de aplicativos front-end baseados na web** – foco na determinação da usabilidade, acessibilidade e conformidade em aplicativos financeiros, incluindo compatibilidade entre navegadores, tratamento de conteúdo dinâmico, limitações/instabilidade da automação da GUI e automação de testes com navegadores headless.

- **Automação do backend** – com foco na integridade dos dados, integração e lógica de negócios em sistemas financeiros, incluindo complexidades de integração de APIs, garantia da integridade dos dados e defeitos de balanceamento de carga e escalabilidade.
- **Testes de segurança automatizados** – no setor financeiro, relacionados a:
  - mascaramento obrigatório de dados confidenciais,
  - alto nível de resultados de teste com falsos positivos e falsos negativos, e a necessidade de verificação manual periódica dos resultados do teste das ferramentas de segurança,
  - trabalho com tráfego criptografado e autenticação.

A automação de testes traz imensos benefícios para o desenvolvimento de software financeiro, mas acarreta desafios significativos relacionados a componentes móveis, front-end e back-end.

As atividades para superar esses desafios incluem:

- a adoção de uma pirâmide de teste baseada em riscos,
- gerenciamento de dados de teste e isolamento de ambientes em CI/CD,
- reduzir a instabilidade d com localizadores de confiabilidade elevada, esperas explícitas, configuração/desmontagem idempotentes,
- definir uma matriz de dispositivos/redes, aproveitar nuvens de dispositivos e dar preferência a frameworks de plataforma para garantir estabilidade — aplicável a testes móveis.

A automação de testes em software financeiro tem grande potencial para melhorar a eficiência e ajudar a garantir a qualidade dos serviços financeiros. A GenAI é promissora para a automação de testes financeiros, oferecendo cobertura abrangente de testes, detecção de defeitos, automação de tarefas e feedback rápido. Para concretizar esse potencial, é necessário superar os desafios descritos.

7 Lista de Abreviações

	Definição
AML	Combate à Lavagem de Dinheiro
Basileia III / IV	Conjunto de medições acordadas internacionalmente pelo Comitê de Supervisão Bancária de Basileia
CAC	Conformidade Automatizada Contínua
CACV	Validação Automática e Contínua da Conformidade
CAMT	Gestão de Caixa (categoria de mensagem ISO 20022)
CCM	Gestão Contínua da Conformidade
CFT	Combate ao Financiamento do Terrorismo
CTFL	Testador Certificado - Nível Básico
CT-FT	Testador Certificado - Teste Financeiro
CPU	Unidade Central de Processamento
DAST	Teste Dinâmico de Segurança de Aplicações
DORA	Lei de Resiliência Operacional Digital
DTO	Objeto de Transferência de Dados
EMS	Sistema de Gerenciamento de Execução
RGPD	Regulamento Geral sobre a Proteção de Dados
GenAI	Inteligência Artificial Generativa
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
ISO	Organização Internacional de Normalização
KYC	Conheça o seu cliente
MiCA	Regulamento dos Mercados de Criptoativos
MFA	Autenticação Multifatorial
MTBF	Tempo médio entre falhas
MTTF	Tempo médio até a falha
MTTR	Tempo médio de reparo
OMS	Sistema de gerenciamento de pedidos
OWASP	Projeto Aberto Mundial de Segurança de Aplicações
PACS	Compensação e Liquidação de Pagamentos (categoria de mensagem ISO 20022)
PAIN	Iniciação de Pagamento (categoria de mensagem ISO 20022)
PAN	Número de conta principal do dispositivo
PCI DSS	Padrão de Segurança de Dados da Indústria de Cartões de Pagamento
PII	Informações de Identificação Pessoal
POS	Ponto de Venda
PSD2	Diretiva de Serviços de Pagamento 2 da União Europeia
RTO	Objetivo de Tempo de Recuperação
RPO	Objetivo de Ponto de Recuperação

SAST	Static Application Security Testing
SCA	Autenticação Forte do Cliente
SOX	Lei Sarbanes-Oxley
SUT	Sistema em Teste

8 Termos específicos de domínios não relacionados a testes

Nome do termo	Definição
trilha de auditoria	Um sistema que rastreia as transações detalhadas relacionadas a qualquer item em um registro contábil.
Basileia III / IV	Um framework regulatório internacional para bancos que reforça os requisitos de capital, torna mais rigorosas as regras de risco e liquidez e exige relatórios precisos e submetidos a auditoria.
risco de conformidade	O risco de sanções legais, perdas financeiras ou danos à reputação que uma instituição pode sofrer como resultado da falha no cumprimento de leis, regulamentos, códigos de conduta e padrões de melhores práticas.
confiança do cliente	A confiança que um consumidor deposita em uma empresa para que esta cumpra seus compromissos e mantenha suas promessas.
precisão dos dados	Uma medição do grau de correspondência entre as informações e os objetos ou eventos que estão sendo registrados.
violação de dados	Um incidente de segurança em que informações confidenciais ou sensíveis são acessadas, visualizadas, divulgadas, copiadas ou roubadas ilegalmente por um indivíduo ou grupo não autorizado, comprometendo sua segurança, integridade ou confidencialidade.
consistência dos dados	A precisão, integridade e exatidão dos dados armazenados em um banco de dados
privacidade do dado	A privacidade do dado refere-se à proteção de informações pessoais contra acesso, divulgação, alteração ou destruição não autorizados. Envolve políticas, procedimentos e tecnologias que regem a forma como os dados privados dos indivíduos são coletados, armazenados, processados e compartilhados pelas organizações.
perfil de dados	A análise, o exame e a síntese sistemáticos de conjuntos de dados para compreender sua estrutura, conteúdo, relações e qualidade.
reconciliação de dados	O processo sistemático de comparar dados de diferentes fontes para determinar a precisão dos dados, a consistência dos dados e a integridade.
Digital Operational Resilience Act (DORA)	Regulamentação que reforça a resiliência operacional das tecnologias da informação e comunicação (TIC) e dos prestadores de serviços terceirizados no setor financeiro da UE.
Data Transfer Object (DTO)	Um padrão de projeto utilizado no desenvolvimento de software para transferir dados de forma eficiente entre diferentes camadas ou componentes de um aplicativo. Normalmente, contém apenas os campos necessários para a transferência de informações, sem qualquer lógica de negócios ou comportamento, garantindo a

Nome do termo	Definição
	separação de responsabilidades e melhorando a performance ao minimizar o tráfego de rede.
instituição financeira	Uma empresa ou organização que realiza transações financeiras e monetárias, atuando como intermediária para fornecer serviços financeiros, tais como empréstimos, depósitos, investimentos e seguros a pessoas físicas, empresas e governos.
GenAI	A Inteligência Artificial Generativa (GenAI) é um ramo da inteligência artificial que utiliza grandes modelos pré-treinados para gerar resultados semelhantes aos humanos, como texto, imagens ou código. Os Large Language Models (LLMs) são modelos GenAI pré-treinados em grandes conjuntos de dados textuais, permitindo-lhes determinar o contexto e produzir respostas relevantes de acordo com as solicitações do usuário.
General Data Protection Regulation (GDPR)	Um regulamento da União Europeia (UE) que estabelece regras abrangentes para a privacidade do dado e a proteção de dados pessoais dos residentes.
Lei Geral de Proteção de Dados Pessoais (LGPD)	Lei nº 13.709/2018 da legislação federal brasileira, criada para regulamentar o tratamento de dados pessoais de cidadãos por pessoas físicas ou jurídicas, públicas ou privadas.
contabilidade geral	O sistema contábil central e principal de uma empresa, utilizado para registrar todas as suas transações financeiras em várias contas, como ativos, passivos, patrimônio líquido, receitas e despesas.
know your customer (KYC)	Um processo obrigatório para instituições financeiras verificarem a identidade de seus clientes e avaliarem riscos potenciais.
Open Web Application Security Project (OWASP)	Fundação sem fins lucrativos que trabalha para melhorar a segurança de software.
Payment Card Industry Data Security Standard (PCI DSS)	Um conjunto de normas de segurança que qualquer empresa que lida com dados de cartões de crédito ou débito deve seguir para prevenir fraudes.
Avaliação de risco periódica	Uma revisão programada e recorrente das operações, sistemas ou projetos de uma organização para identificar, analisar e mitigar ameaças em evolução.
privacidade	O direito de proteger suas informações pessoais, seu espaço e suas comunicações contra invasões e observações não autorizadas.
PSD2	Diretiva de Serviços de Pagamento 2. Uma diretiva da UE que regula os serviços de pagamento para aumentar a concorrência, melhorar a segurança e abrir o mercado a novas empresas, conhecidas como prestadores de serviços terceirizados.
conformidade regulatória	O processo pelo qual uma organização segue as leis, regulamentos, normas e regras aplicáveis estabelecidos por governos e órgãos reguladores para apoiar operações legais, éticas e seguras.

Nome do termo	Definição
norma regulatória	Regra ou requisito oficial estabelecido por um governo ou outra autoridade para determinar níveis mínimos de qualidade, segurança ou performance em um setor ou processo.
transferência de risco	
sistema de liquidação	Conjunto de processos, regras e infraestrutura que permite a transferência final de dinheiro ou títulos para cumprir uma obrigação financeira entre as partes.
Lei Sarbanes-Oxley (SOX)	Lei federal dos Estados Unidos que exige que as empresas de capital aberto estabeleçam e mantenham registros financeiros precisos e controles internos robustos para prevenir fraudes corporativas e proteger os investidores.

9 Referências

9.1 Normas

ISO 20022 Financial services – Universal financial industry message scheme (2025)

https://www.iso20022.org/

ISO/IEC 25010 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) System and software quality models (2023)

https://iso25000.com/index.php/en/iso-25000-standards/iso-25010

ISO/IEC 25019:2023 Systems and software engineering

https://www.iso.org/standard/78177.html

ISO/IEC 27001 Information security, cybersecurity and privacy protection – Information security management systems – Requirements (2022)

https://www.iso.org/standard/27001

IS0 31000 Risk management – Principles and guidelines (2018)

https://www.iso.org/standard/65694.html

MiFID II Markets in Financial Instruments Directive II, European Union (2018)

https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng

OWASP The Open Worldwide Application Security Project (2021)

https://owasp.org/

PSD2 Revised Payment Services Directive 2, European Union (2019)

https://www.ecb.europa.eu/press/intro/mip-online/2018/html/1803_revisedpsd.en.html

9.2 ISTQB® Documentos

[ISTQB_CTAL-TA_SYL] ISTQB® Advanced Level Test Analyst Syllabus, V4.0, 2025, https://istqb.org/wp-content/uploads/sdm-uploads/ISTQB-CTAL-TA-Syllabus-v4.0-EN-4.pdf

[ISTQB_CTAL-TAE_SYL] ISTQB® Certified Tester Advanced Level Test Automation Engineering, v2.0, 2024, https://istqb.org/certifications/certified-tester-advanced-level-test-automation-engineering-ctal-tae-v2-0/

[ISTQB_CT-ATLaS_SYL] ISTQB® Certified Tester Agile Test Leadership at Scale (ATLaS) v2.0, 2023, https://istqb.org/wp-content/uploads/2024/11/ISTQB_CT-ATLaS_Syllabus_v2.0.pdf

[ISTQB_CT-GenAI_SYL] ISTQB® Certified Tester Testing with Generative AI v1.0, 2025, https://istqb.org/wp-content/uploads/sdm-uploads/CT-GenAI-Syllabus-v1.0.pdf

[ISTQB_CTFL_SYL] ISTQB® Foundation Level Syllabus v4.0.1, 2024, https://istqb.org/wp-content/uploads/2024/11/ISTQB_CTFL_Syllabus_v4.0.1.pdf

[ISTQB_CT-MAT] ISTQB® Certified Tester Mobile Application Testing, https://istqb.org/wp-content/uploads/2024/11/ISTQB-CT-MAT_Syllabus_v1.0_2019.pdf

[ISTQB_CT-PT_SYL] ISTQB® Certified Tester Performance Testing, v1.0, 2018, https://istqb.org/wp-content/uploads/2024/11/ISTQB-CT-PT_Syllabus_v1.0_2018.pdf

[ISTQB_CT-SEC_SYL] ISTQB® Security Tester v1.0, 2016, https://istqb.org/wp-content/uploads/2024/11/ISTQB-CT-SEC_Syllabus_v1.0_2016.pdf

[ISTQB_CT-STE_SYL] ISTQB® Security Test Engineer v1.0.1, 2025, https://istqb.org/certifications/certified-tester-security-test-engineer/

[ISTQB_CT-TAS_SYL] ISTQB® Certified Tester Test Automation Strategy v1.0, 2024, https://istqb.org/wp-content/uploads/2024/11/ISTQB_CT-TAS_Syllabus_v1.0.pdf

9.3 Referências do Glossário

- Agile Alliance https://www.agilealliance.org/agile-practice-guide/
- IREB-CPRE para Engenharia de Requisitos https://www.ireb.org/en/cpre/glossary
- Glossário ISTQB® https://glossary.istqb.org/

9.4 Livros, artigos e páginas da Web

Livros

Adzic, G. (2009). Bridging the Communication Gap: Specification by Example and Agile Acceptance Testing. Neuri Limited.

Adzic, G. (2009b). Test Driven Development: By Example. Addison-Wesley.

Enders, A. (1975). An Analysis of Errors and Their Causes in System Programs. IEEE Transactions on Software Engineering, pp. 140-149.

Marick, B. (2003). Exploration through Example. Retrieved from http://www.exampler.com/old-blog/2003/08/21.1.html#agile-testing-project-1

Páginas da Web

Dieu (2024) Linh Chu Dieu, “Best QA and Testing Practices for Financial Systems”, from https://smartdev.com/best-qa-and-testing-practices-for-financial-systems/

Hayes (2025) Adam Hayes, “What Is a Financial Institution”, from https://www.investopedia.com/terms/f/financialinstitution.asp

Joseph (2020) Timothy Joseph. “Financial Domain Testing: The Breakdown”, from https://blog.qasource.com/financial-domain-testing-the-breakdown/

Veenendaal (2012) “PRISMA: Product Risk Assessment for Agile projects”, from https://www.erikvanveenendaal.nl/NL/files/testing_experience_no_20_column_van_veenendaal.pdf

The previous references point to information available on the Internet and elsewhere. Even though those references were checked at the time of publication of this syllabus, the ISTQB® cannot be held responsible if the references are not available anymore.

Apêndice A – Objetivos de Aprendizagem/Nível Cognitivo de Conhecimento

Os objetivos de aprendizagem específicos aplicáveis a este syllabus são apresentados no início de cada capítulo. Cada tópico do syllabus será examinado de acordo com seu objetivo de aprendizagem.

Os objetivos de aprendizagem começam com um verbo de ação correspondente ao seu nível cognitivo de conhecimento, conforme listado abaixo.

Nível 1: Lembrar (K1)

O candidato irá lembrar, reconhecer e recordar um termo ou conceito.

Verbos de ação: Recordar, reconhecer.

Exemplos
Recordar os conceitos da piramide de teste.
Reconhecer os objetivos típicos dos testes.

Nível 2: Compreender (K2)

O candidato é capaz de identificar as razões ou explicações para afirmações relacionadas ao tema, resumir, comparar, classificar e dar exemplos sobre o conceito em questão.

Verbos de ação: Classificar, comparar, diferenciar, distinguir, explicar, dar exemplos, interpretar, resumir

Exemplos	**Notas**
Classifique as ferramentas de teste de acordo com sua finalidade e as atividades de teste que elas suportam.	
Comparar os diferentes níveis de teste.	Pode ser usado para procurar semelhanças, diferenças ou ambos.
Diferenciar teste de depuração.	Procure diferenças entre conceitos.
Distinguir entre riscos de projeto e riscos de produto.	Permite que dois (ou mais) conceitos sejam classificados separadamente.
Explique o impacto do contexto no processo de teste.	
Dê exemplos de por que o teste é necessário.	
Inferir a causa-raiz dos defeitos a partir de um determinado perfil de falhas.	
Resumir as atividades do processo de revisão do produto de trabalho.	

Nível 3: Aplicar (K3)

O candidato é capaz de executar um procedimento quando confrontado com uma tarefa familiar, ou selecionar o procedimento correto e aplicá-lo a um determinado contexto.

Verbos de ação: Aplicar, implementar, preparar, usar

Exemplos	Notas
Aplicar a análise de valor limite para derivar casos de teste a partir de requisitos dados.	Deve consultar um procedimento/técnica/processo, etc.
Implementar métodos de coleta de métricas para atender aos requisitos técnicos e de gestão.	
Prepare testes de instalabilidade para aplicativos móveis.	
Use a rastreabilidade para monitorar o progresso dos testes quanto à integridade e consistência com os objetivos do teste, a estratégia de teste e o plano de teste.	Pode ser usado em um LO que deseja que o candidato seja capaz de usar uma técnica ou procedimento. Semelhante a “aplicar”.

Referência

(Para os níveis cognitivos dos objetivos de aprendizagem)

Anderson, L. W. e Krathwohl, D. R. (eds) (2001) A Taxonomy for Learning, Teaching and

Avaliação: Uma Revisão da Taxonomia de Objetivos Educacionais de Bloom, Allyn and Bacon

Apêndice B – Matriz de rastreabilidade de Resultados de Negócios com Objetivos de Aprendizagem

Esta seção lista a rastreabilidade entre os Resultados de Negócios e os Objetivos de Aprendizagem do Teste de Certificação - Testes Financeiros.

Resultados de Negócios: Certified Tester - Finance Testing			BO1	BO2	BO3	RO4	BO5	BO6
BO1	Compreender a estrutura do setor financeiro, suas instituições, sistemas e processos, e explicar os desafios específicos dos testes nesse domínio.		4					
BO2	aplicar práticas de testes que apoiem a conformidade com regulamentos e normas financeiras, garantindo que os requisitos de auditabilidade, rastreabilidade e documentação sejam atendidos.			7				
BO3	aplicar testes baseados em riscos aos sistemas financeiros, priorizando as atividades de teste de acordo com os riscos comerciais, técnicos e regulatórios.				3			
BO4	compreender as práticas de teste que garantem a precisão dos dados, a consistência dos dados e a proteção dos dados em todos os sistemas financeiros, incluindo o uso de técnicas de mascaramento e anonimização.					4		
BO5	aplicar técnicas de teste funcionais e não funcionais no domínio financeiro, com ênfase especial no desempenho, na confiabilidade e na segurança.						5	
BO6	compreender o papel da automação de testes em ambientes financeiros e aplicar estratégias de automação de testes de forma eficaz tanto em sistemas legados quanto em sistemas modernos, levando em consideração as restrições regulatórias.							4
LO exclusivo	Objetivo de Aprendizagem	Nível K						
1	Introdução ao setor de serviços financeiros							
1.1	Fundamentos do teste de software em testes financeiros							

FT-1.1.1	Lembre-se dos principais objetivos dos testes financeiros	K1	X					
FT-1.1.2	Resumir as características únicas e os requisitos técnicos de vários ambientes de teste financeiros	K2	X					
FT-1.1.3	Identificar os principais sistemas financeiros e os fluxos de trabalho típicos com testabilidade associados a eles	K2	X					
1.2	Desafios e o papel do conhecimento de domínio nos testes financeiros							
FT-1.2.1	Explique como o conhecimento de domínio é aplicado para mitigar desafios comuns de testes no setor financeiro	K2	X					
2	Teste de conformidade							
2.1	Objetivos e abordagens dos testes de conformidade							
FT-2.1.1	Resumir os objetivos dos testes de conformidade e a relação entre suas principais abordagens de teste	K2		X				
2.2	Regulamentos financeiros e seu impacto nos testes							
FT-2.2.1	Explique a relevância das principais regulamentações e normas financeiras para os testes	K2		X				
FT-2.2.2	Recordar as consequências da não conformidade com as regulamentações financeiras	K1		X				
2.3	Características distintivas dos testes de finanças regulamentadas							
FT-2.3.1	Resumir as características únicas dos testes financeiros	K2		X				
2.4	Auditabilidade e validação contínua e automatizada da conformidade							
FT-2.4.1	Compreender os princípios fundamentais da auditabilidade em testes de conformidade	K2		X				
FT-2.4.2	Compreender os princípios e mecanismos de implementação da Validação Automática Contínua de Conformidade (CACV) no ciclo de vida de entrega de software.	K2		X				
3	Testes Baseados em Riscos							
3.1	Categorias de risco nos sistemas financeiros							
FT-3.1.1	Explique as principais categorias de risco nos sistemas financeiros	K2			X			
3.2	Princípios de testes baseados em riscos em finanças							

FT-3.2.1	Explicar os princípios dos testes baseados em riscos em finanças	K2			X			
3.3	Atividades baseadas no risco							
FT-3.3.1	Explique como a priorização baseada em risco afeta as atividades de teste em aplicativos financeiros	K2			X			
4	Teste de dados e gerenciamento de dados							
4.1	Precisão e consistência dos dados							
FT-4.1.1	Explique a importância da precisão dos dados e da consistência dos dados em todos os sistemas financeiros	K2				X		
4.2	Reconciliação de dados entre sistemas financeiros							
FT-4.2.1	Aplicar técnicas de reconciliação de dados a processos financeiros multissistemas	K3				X		
4.3	Privacidade do dado e proteção de dados em testes financeiros							
FT-4.3.1	Explique a importância da privacidade do dado e da proteção de dados em testes financeiros	K2				X		
5	Teste Funcional e Teste Não Funcional							
5.1	Teste funcional de sistemas financeiros							
FT-5.1.1	Aplicar técnicas de teste funcional para validar sistemas financeiros	K3					X	
5.2	Riscos de performance em finanças							
FT-5.2.1	Explique os riscos de performance em sistemas financeiros durante períodos de pico	K2					X	
5.3	Teste de performance em contextos financeiros							
FT-5.3.1	Aplicar testes de carga e testes de estresse em contextos específicos da área financeira	K3					X	
5.4	Teste de segurança e de disponibilidade							
FT-5.4.1	Explicar as necessidades de testes de segurança e disponibilidade em sistemas financeiros	K2					X	
5.5	GenAI em testes de software financeiro							
FT-5.5.1	Explique como a GenAI pode apoiar e melhorar os testes financeiros	K2					X	

6	Automação de testes							
6.1	Papel da automação de testes nos testes financeiros							
FT-6.1.1	Explique como a automação de testes contribui para a eficiência dos testes na área financeira	K2						X
6.2	Estratégias de automação de testes							
FT-6.2.1	Aplicar estratégias de automação de testes em ambientes de TI financeiros legados e modernos	K3						X
6.3	Desafios da automação de testes em ambientes regulamentados							
FT-6.3.1	Explique os desafios da automação de testes em ambientes regulamentados	K2		X				X
6.4	Desafios em diferentes tipos de automação de testes							
FT-6.4.1	Explique os desafios da automação de testes em componentes móveis, front-end e back-end	K2						X

Apêndice C – Notas de Lançamento

O ISTQB® Certified Tester – Finance Testing (CT-FT) Syllabus v1.0 é a primeira versão deste syllabus especializado. Ele apresenta uma abordagem estruturada para testes no domínio financeiro, abordando os desafios específicos dos sistemas financeiros, processos e requisitos regulatórios.

A criação deste syllabus foi motivada pela crescente dependência de ambientes de TI complexos no setor financeiro, pela importância cada vez maior da conformidade regulatória e pela demanda por abordagens de teste baseadas em riscos e focadas em dados.

Esta versão tem como objetivo fornecer às organizações financeiras, testadores e profissionais de qualidade conhecimentos práticos e específicos do domínio que complementam o portfólio existente do ISTQB®.

Objetivo e benefícios

O syllabus CT-FT fortalece o portfólio do ISTQB®ao abordar um dos setores mais regulamentados e críticos do mundo. Ele permite que os testadores adquiram valiosa expertise no domínio, apoia as organizações no cumprimento de requisitos de conformidade e qualidade e contribui para o reconhecimento profissional dos testes financeiros em todo o mundo.

Como primeira versão, o CT-FT estabelece a base para futuras atualizações. As evoluções acompanharão as tendências do setor, os avanços regulatórios e as tecnologias emergentes, a fim de garantir que o syllabus continue sendo relevante tanto para os profissionais quanto para as organizações.

Apêndice D – Índice