

Certified Tester Finance Testing (CT-FT) Syllabus

v1.0

International Software Testing Qualifications Board



Avviso di Copyright

Avviso di copyright © International Software Testing Qualifications Board (di seguito denominato ISTQB®)

ISTQB® è un marchio registrato di International Software Testing Qualifications Board.

Copyright © 2026, gli autori 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.

Tutti i diritti riservati. Con la presente gli autori trasferiscono il copyright a ISTQB®. Gli autori (come attuali titolari del copyright) e ISTQB® (come futuro titolare del copyright) hanno concordato le seguenti condizioni di utilizzo:

È possibile copiare estratti di questo documento per uso non commerciale, a condizione che venga riconosciuta la fonte. Qualsiasi Training Provider accreditato può utilizzare questo syllabus come base per un corso di formazione, a condizione che gli autori e ISTQB® siano riconosciuti come fonte e titolari del copyright del syllabus e a condizione che qualsiasi pubblicità di tale corso di formazione possa menzionare il syllabus solo dopo aver ricevuto l'accREDITAMENTO ufficiale dei materiali di formazione da un Member Board riconosciuto da ISTQB®.

Qualsiasi individuo o gruppo di individui può utilizzare questo syllabus come base per articoli e libri, a condizione che gli autori e ISTQB® siano riconosciuti come fonte e titolari del copyright del syllabus.

È proibito qualsiasi altro utilizzo di questo syllabus senza aver prima ottenuto l'approvazione scritta di ISTQB®.

Qualsiasi Member Board riconosciuto da ISTQB® può tradurre questo syllabus a condizione che riproduca il suddetto avviso di copyright nella versione tradotta del syllabus.

Cronologia delle Revisioni

Versione	Data	Osservazioni
v1.0	30/09/2025	Alpha review
v1.0	01/02/2026	Beta review
v1.0	17/04/2026	Versione di rilascio

Cronologia delle versioni della traduzione italiana del syllabus v1.0

Versione	Data	Osservazioni
Ver. A	14/09/2026	Prima versione pubblicata della traduzione italiana

Nota del traduttore

Nella tabella «Termini Specifici del Dominio non Relativi al Testing» (Capitolo 8) il termine «trasferimento del rischio» («risk transfer») è riportato senza definizione, perché la definizione manca anche nel documento originale inglese. A beneficio del lettore se ne propone qui una formulazione a cura del traduttore, che non costituisce una definizione ufficiale approvata da ISTQB®:

trasferimento del rischio — Strategia di gestione del rischio che sposta su una terza parte, per esempio mediante una polizza assicurativa o una clausola contrattuale, l'onere economico delle conseguenze di un rischio. La responsabilità verso l'autorità di vigilanza per la conformità resta comunque in capo all'istituto.

Indice dei Contenuti

Avviso di Copyright	2
Cronologia delle Revisioni.....	3
Indice dei Contenuti	4
Ringraziamenti	7
0 Introduzione	8
0.1 Scopo di questo Syllabus	8
0.2 Il Certified Tester - Finance Testing di ISTQB® nel Testing del Software	8
0.3 Percorso di Carriera per i Tester	8
0.4 Business Outcome	9
0.5 Obiettivi di Apprendimento e Livello Cognitivo di Conoscenza	9
0.6 L'Esame per il Certificato Certified Tester - Finance Testing	10
0.7 Accreditamento	10
0.8 Gestione degli Standard	10
0.9 Livello di Dettaglio.....	11
0.10 Com'è Organizzato questo Syllabus.....	11
1 Introduzione al Settore dei Servizi Finanziari – 50 minuti	13
Introduzione al Settore dei Servizi Finanziari.....	14
1.1 Fondamenti del Testing del Software nei Servizi Finanziari.....	14
1.1.1 Definizione e Obiettivi del Finance Testing	14
1.1.2 Tipi di Ambienti di Test Finanziari negli Istituti Finanziari	14
1.1.3 Architetture dei Sistemi Finanziari e Workflow Testabili	15
1.2 Sfide e Ruolo della Conoscenza del Dominio nel Finance Testing.....	16
2 Testing di Conformità – 80 minuti.....	18
Testing di Conformità	19
2.1 Obiettivi e Approcci del Testing di Conformità.....	19
2.2 Le Normative Finanziarie e il Loro Impatto sul Testing	20
2.2.1 Principali Normative Finanziarie e Loro Rilevanza per il Testing	20
2.2.2 Conseguenze della Non-Conformità	21
2.3 Caratteristiche Distintive del Finance Testing Regolamentato	21
2.4 Auditability e Validazione Continua Automatizzata della Conformità	22
2.4.1 Auditability	22

Syllabus-Finance Testing (CT-FT)

2.4.2	Validazione Continua Automatizzata della Conformità	23
3	Testing Basato sul Rischio – 45 minuti	25
	Introduzione al Testing Basato sul Rischio nei Sistemi Finanziari.....	26
3.1	Categorie di Rischio nei Sistemi Finanziari	26
3.2	Principi del Testing Basato sul Rischio nei Sistemi Finanziari	27
3.3	Attività di Test Relative al Testing Basato sul Rischio.....	28
4	Testing dei Dati e Gestione dei Dati – 90 minuti	30
	Introduzione al Testing dei Dati e alla Gestione dei Dati	31
4.1	Accuratezza dei Dati e Consistenza dei Dati.....	31
4.2	Riconciliazione dei Dati tra Sistemi Finanziari.....	32
4.3	Data Privacy e Protezione dei Dati nel Finance Testing	33
5	Testing Funzionale e Non-Funzionale – 165 minuti	36
	Introduzione al Testing Funzionale e Non-Funzionale	37
5.1	Testing Funzionale dei Sistemi Finanziari	37
5.2	Rischi di Prestazione in Ambito Finanziario	39
5.3	Performance Testing in Contesti Finanziari.....	40
5.4	Testing di Sicurezza e Testing di Disponibilità	41
5.5	GenAI nel Testing del Software Finanziario	43
6	Test Automation – 105 minuti.....	45
	Introduzione alla Test Automation	46
6.1	Ruolo della Test Automation nel Finance Testing	46
6.2	Strategie di Test Automation	47
6.3	Sfide della Test Automation in Ambienti Regolamentati	48
6.4	Sfide nei Diversi Tipi di Test Automation.....	49
7	Elenco delle Abbreviazioni	51
8	Termini Specifici del Dominio non Relativi al Testing	53
9	Riferimenti	56
9.1	Standard	56
9.2	Documenti ISTQB®	56
9.3	Riferimenti al Glossario.....	57
9.4	Libri, Articoli e Pagine Web.....	57
	Appendice A – Obiettivi di Apprendimento/Livello Cognitivo di Conoscenza	59
	Livello 1: Ricordare (K1)	59

Syllabus-Finance Testing (CT-FT)

Livello 2: Comprendere (K2).....	59
Livello 3: Applicare (K3).....	60
10 Appendice B – Matrice di Tracciabilità dei Business Outcome rispetto agli Obiettivi di Apprendimento	61
11 Appendice C – Note di Rilascio	65
12 Appendice D – Indice Analitico.....	66

Ringraziamenti

Questo documento è stato rilasciato ufficialmente dall'Assemblea Generale di ISTQB® il 17 aprile 2026

È stato prodotto da un team dell'International Software Testing Qualifications Board: Florian Fieber (presidente), Richard Seidl (vicepresidente), 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.

Il team ringrazia i Member Board per i loro suggerimenti e contributi.

Le seguenti persone hanno partecipato alla review, ai commenti e alla votazione di questo 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 (Glossary WG), 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 (Exam WG), Tanja Tremmel (GTB), Taz Daughtrey (ASTQB), Vinicius Pazutti Correia (DSTB), Walter Eder (ATB)

Traduzione italiana a cura di ITA-STQB (www.ita-stqb.org) – info@ita-stqb.org

0 Introduzione

0.1 Scopo di questo Syllabus

Questo syllabus costituisce la base per la qualifica *ISTQB® Certified Tester – Finance Testing* (CT-FT). È destinato a chi lavora nei sistemi finanziari o con essi ed è coinvolto nel testing del software e nella Quality Assurance in questo dominio. ISTQB® mette a disposizione questo syllabus per:

- i Member Board, affinché lo traducano nella propria lingua e accreditino i training provider. I Member Board possono adattare il syllabus alle specifiche esigenze linguistiche e modificare i riferimenti per adeguarli alle pubblicazioni locali.
- gli enti di certificazione, affinché ne derivino le domande d'esame nella propria lingua, adattate agli obiettivi di apprendimento di questo syllabus.
- i training provider, affinché producano i materiali di formazione e determinino i metodi didattici appropriati.
- i candidati alla certificazione, affinché si preparino all'esame di certificazione (sia nell'ambito di un corso di formazione sia autonomamente).
- la comunità internazionale dell'ingegneria del software e dei sistemi, per far progredire la professione del testing del software e dei sistemi e come base per libri e articoli.

0.2 Il Certified Tester - Finance Testing di ISTQB® nel Testing del Software

La qualifica ISTQB® Certified Tester – Finance Testing (CT-FT) si rivolge ai professionisti coinvolti nel testing del software o nella Quality Assurance all'interno di istituti finanziari, aziende di tecnologia finanziaria (fintech) o organismi di regolamentazione. È adatta, ad esempio, a tester, business analyst, sviluppatori, compliance officer, auditor e regolatori che desiderano comprendere i requisiti specifici di testing e di conformità dei sistemi finanziari.

La certificazione fornisce un'estensione focalizzata sul dominio rispetto alla qualifica Foundation Level (CTFL), approfondendo la comprensione da parte del candidato dei temi normativi, di rischio, di dati, di sicurezza, di automazione e di prestazione specifici del settore finanziario.

0.3 Percorso di Carriera per i Tester

Lo schema ISTQB® supporta i professionisti del testing in tutte le fasi della loro carriera, offrendo ampiezza e profondità di conoscenza. Chi consegue la certificazione ISTQB® Certified Tester - Finance Testing può essere interessato anche ai Core Advanced Level (Test Analyst, Technical Test Analyst e Test Management, Test Automation Engineer) e successivamente all'Expert Level (Test Management o Improving the Test Process). Lo stream Specialist offre un approfondimento su aree che hanno approcci del test e attività di test specifici, ad esempio Agile Testing, AI Testing o Mobile App Testing, oppure che raccolgono il know-how di testing di determinati domini industriali, ad esempio Gambling o Gaming. Per le informazioni più aggiornate sullo schema ISTQB® Certified Tester si rimanda a www.istqb.org.

0.4 Business Outcome

Questa sezione elenca i Business Outcome attesi da un candidato che ha conseguito la certificazione Certified Tester - Finance Testing.

Un Certified Tester in Finance Testing è in grado di...

BO1	comprendere la struttura del settore finanziario, i suoi istituti, sistemi e processi e spiegare le sfide specifiche del testing all'interno di questo dominio.
BO2	applicare pratiche di test che supportano la conformità alle normative e agli standard finanziari, verificando che siano soddisfatti i requisiti di auditability, tracciabilità e documentazione.
BO3	applicare il testing basato sul rischio ai sistemi finanziari, prioritizzando le attività di test in base ai rischi di business, tecnici e normativi.
BO4	comprendere le pratiche di test che verificano l'accuratezza, la consistenza e la protezione dei dati nei sistemi finanziari, incluso l'uso di tecniche di masking e di anonimizzazione.
BO5	applicare le tecniche di test funzionali e non-funzionali tipicamente utilizzate nel dominio finanziario, con particolare attenzione agli aspetti non-funzionali quali prestazioni, affidabilità e sicurezza.
BO6	comprendere il ruolo della test automation negli ambienti finanziari e applicare efficacemente le strategie di test automation sia nei sistemi legacy sia in quelli moderni, tenendo conto dei vincoli normativi.

(Vedere la mappatura completa nell'Appendice B).

0.5 Obiettivi di Apprendimento e Livello Cognitivo di Conoscenza

Gli obiettivi di apprendimento supportano i business outcome e vengono utilizzati per creare gli esami Certified Tester - Finance Testing.

Le domande d'esame verificheranno la conoscenza delle parole chiave a livello K1 (vedi sotto) o degli obiettivi di apprendimento al rispettivo livello di conoscenza.

Gli obiettivi di apprendimento specifici e i relativi livelli di conoscenza sono indicati all'inizio di ogni capitolo e sono classificati come segue:

- K1: Ricordare
- K2: Comprendere
- K3: Applicare

Ulteriori dettagli ed esempi di obiettivi di apprendimento sono riportati nell'Appendice A.

Per tutti i termini elencati come parole chiave appena sotto i titoli dei capitoli, è necessario ricordare il nome corretto e la definizione dal glossario ISTQB® (K1), anche se non esplicitamente menzionati nell'obiettivo di apprendimento.

0.6 L'Esame per il Certificato Certified Tester - Finance Testing

L'esame per il certificato Certified Tester - Finance Testing sarà basato su questo syllabus. Le risposte alle domande d'esame possono richiedere l'utilizzo di materiale basato su più di una sezione di questo syllabus. Tutte le sezioni del syllabus sono esaminabili, a eccezione dell'Introduzione e delle Appendici. Standard e libri sono inclusi come riferimenti, ma il loro contenuto non è esaminabile, oltre a quanto riassunto nel syllabus stesso a partire da tali standard e libri.

Per ulteriori dettagli si rimanda al documento Certified Tester - Finance Testing Exam Structures and Rules V1.0.

Per poter accedere all'esame Finance Testing (CT-FT), i candidati devono essere in possesso di un certificato ISTQB® Certified Tester Foundation Level (CTFL) valido.

La familiarità con i sistemi finanziari o con i progetti software del dominio finanziario è utile ma non obbligatoria.

0.7 Accredитamento

Un Member Board ISTQB® può accreditare i training provider il cui materiale didattico segue questo syllabus. I training provider dovrebbero ottenere le linee guida per l'accreditamento dal Member Board o dall'organismo che effettua l'accreditamento. Un corso accreditato è riconosciuto come conforme a questo syllabus ed è autorizzato a prevedere un esame ISTQB® come parte del corso.

Le linee guida per l'accreditamento di questo syllabus seguono le Accreditation Guidelines generali pubblicate dal Processes Management and Compliance Working Group.

0.8 Gestione degli Standard

Organizzazioni internazionali di standardizzazione come IEEE e ISO hanno emesso standard relativi alle caratteristiche di qualità e al testing del software. Tali standard sono richiamati in questo syllabus. Lo scopo di questi riferimenti è fornire un framework (come nei riferimenti a ISO 25010 relativi alle caratteristiche di qualità) oppure fornire una fonte di informazioni aggiuntive se il lettore lo desidera. Si noti che i syllabus ISTQB® utilizzano i documenti di standard come riferimento. I documenti di standard non sono destinati all'esame.

Il syllabus fa riferimento a normative finanziarie internazionali, standard specifici del dominio e best practice del testing del software. Le fonti principali comprendono:

- la Revised Payment Services Directive 2 (PSD2) dell'Unione Europea, PCI DSS, Basel III / IV e altre linee guida e framework normativi europei
- ISO 20022 Financial services – Universal financial industry message scheme
- ISO 25010 – Product quality model (SQuaRE)
- Open Worldwide Application Security Project (OWASP), ISO 27001 per la sicurezza
- i syllabus ISTQB®

L'elenco completo dei riferimenti è riportato nel Capitolo 9.

0.9 Livello di Dettaglio

Il livello di dettaglio di questo syllabus consente di realizzare corsi ed esami coerenti a livello internazionale. Per raggiungere questo obiettivo, il syllabus è costituito da:

- obiettivi didattici generali che descrivono l'intento del livello Finance Testing
- un elenco di termini che gli studenti devono essere in grado di ricordare
- obiettivi di apprendimento per ciascuna area di conoscenza, che descrivono il risultato cognitivo di apprendimento da conseguire
- una descrizione dei concetti chiave, inclusi i riferimenti a fonti quali letteratura riconosciuta o standard

Il contenuto del syllabus non descrive l'intera area di conoscenza del testing del software; riflette il livello di dettaglio da trattare nei corsi di formazione Certified Tester Finance Testing. Si concentra sugli approcci del test e sulle tecniche di test applicabili a tutti i progetti software in ambito finanziario, inclusi quelli che seguono lo sviluppo software Agile. Questo syllabus non contiene obiettivi di apprendimento specifici relativi al testing Agile, ma tratta il modo in cui questi approcci del test e tecniche di test si applicano ai progetti di sviluppo software Agile e ad altri tipi di progetto.

Il syllabus utilizza la terminologia (cioè il nome e il significato) dei termini usati nel testing del software e nella Quality Assurance secondo il Glossario ISTQB®.

0.10 Com'è Organizzato questo Syllabus

Vi sono sei capitoli con contenuto esaminabile. Il titolo di primo livello di ogni capitolo specifica il tempo dedicato al capitolo; le tempistiche non sono indicate al di sotto del livello di capitolo. *Per i corsi di formazione accreditati, il syllabus richiede un minimo di 8,75 ore di istruzione, distribuite tra i sei capitoli come segue:*

- **Capitolo 1: 50 minuti – Introduzione al Settore dei Servizi Finanziari**
 - Richiamare gli obiettivi primari del finance testing
 - Riassumere le caratteristiche peculiari e i requisiti tecnici dei vari ambienti di test finanziari
 - Identificare i principali sistemi finanziari e i workflow testabili tipicamente associati a essi
 - Spiegare come la conoscenza del dominio viene applicata per mitigare le sfide comuni del testing nel settore finanziario
- **Capitolo 2: 80 minuti – Testing di Conformità**
 - Riassumere gli obiettivi del testing di conformità e la relazione tra i suoi principali approcci del test
 - Spiegare la rilevanza per il testing delle principali normative e standard finanziari
 - Richiamare le conseguenze della non-conformità alle normative finanziarie
 - Riassumere le caratteristiche peculiari del finance testing
 - Comprendere i principi fondamentali dell'auditability nel testing di conformità

- Comprendere i principi e i meccanismi di implementazione della Validazione Continua Automatizzata della Conformità (CACV) all'interno del ciclo di vita di consegna del software
- **Capitolo 3: 45 minuti – Testing Basato sul Rischio**
 - Spiegare le principali categorie di rischio nei sistemi finanziari
 - Spiegare i principi del testing basato sul rischio in ambito finanziario
 - Spiegare come la prioritizzazione basata sul rischio influisce sulle attività di test nelle applicazioni finanziarie
- **Capitolo 4: 90 minuti – Testing dei Dati e Gestione dei Dati**
 - Spiegare l'importanza dell'accuratezza e della consistenza dei dati nei sistemi finanziari
 - Applicare le tecniche di riconciliazione dei dati ai processi finanziari multi-sistema
 - Spiegare l'importanza della data privacy e della protezione dei dati nel finance testing
- **Capitolo 5: 165 minuti – Testing Funzionale e Non-Funzionale**
 - Applicare il testing funzionale per validare i sistemi finanziari
 - Spiegare i rischi di prestazione nei sistemi finanziari durante i periodi di picco
 - Applicare il load testing e lo stress testing in contesti specifici del settore finanziario
 - Spiegare le esigenze di testing di sicurezza e testing di disponibilità nei sistemi finanziari
 - Spiegare come la GenAI può supportare e migliorare il finance testing
- **Capitolo 6: 105 minuti – Test Automation**
 - Spiegare come la test automation supporta l'efficienza dei test in ambito finanziario
 - Applicare le strategie di test automation in panorami IT finanziari legacy e moderni
 - Spiegare le sfide della test automation in ambienti regolamentati
 - Spiegare le sfide della test automation su componenti mobile, frontend e backend

1 Introduzione al Settore dei Servizi Finanziari – 50 minuti

Parole chiave

Parole chiave specifiche del dominio

istituto finanziario, standard normativo

Obiettivi di Apprendimento del Capitolo 1:

1.1 Fondamenti del Testing del Software nel Finance Testing

FT-1.1.1 (K1) Richiamare gli obiettivi primari del finance testing

FT-1.1.2 (K2) Riassumere le caratteristiche peculiari e i requisiti tecnici dei vari ambienti di test finanziari

FT-1.1.3 (K2) Identificare i principali sistemi finanziari e i workflow testabili tipicamente associati a essi

1.2 Sfide e Ruolo della Conoscenza del Dominio nel Finance Testing

FT-1.2.1 (K2) Spiegare come la conoscenza del dominio viene applicata per mitigare le sfide comuni del testing nel settore finanziario

Introduzione al Settore dei Servizi Finanziari

Il settore dei servizi finanziari è il motore principale del commercio globale e va ben oltre la semplice gestione del denaro, abbracciando un ecosistema sofisticato che comprende attività bancarie, assicurative e di investimento. In questo contesto ad alta criticità i sistemi software non sono soltanto strumenti, ma la vera e propria infrastruttura su cui poggiano la stabilità economica e la fiducia del cliente. Con l'accelerazione della trasformazione digitale, il software che alimenta un singolo istituto è diventato inseparabile dalla stabilità dell'economia globale. Questa convergenza fa di un testing del software rigoroso l'unica vera salvaguardia contro un effetto domino causato da un failure sistemico.

1.1 Fondamenti del Testing del Software nei Servizi Finanziari

1.1.1 Definizione e Obiettivi del Finance Testing

Il finance testing è il processo di verifica e validazione delle applicazioni software utilizzate nel settore dei servizi finanziari, che comprende le attività bancarie, la tecnologia finanziaria (fintech), gli istituti finanziari non bancari (NBFIs) — come compagnie assicurative, fondi pensione e società di leasing — e altri servizi finanziari specializzati. Questo testing specifico del dominio valuta se i sistemi finanziari funzionano correttamente, in modo sicuro e in accordo con la logica di business e i requisiti normativi. Comporta la validazione dell'intero ecosistema necessario a erogare i servizi finanziari, in particolare dei workflow software che supportano i processi interni, le interfacce utente esterne e le integrazioni con terze parti.

Gli obiettivi primari del finance testing comprendono:

- Correttezza funzionale – verificare che le transazioni finanziarie, i calcoli matematici complessi (per es. tassi di interesse, ammortamenti) e i saldi dei conti siano elaborati secondo regole di precisione e livelli di tolleranza definiti, per prevenire perdite economiche.
- Conformità normativa – verificare che il software rispetti gli standard legali globali e regionali richiesti, e mitigare il rischio di responsabilità legale e di sanzioni pecuniarie.
- Integrità dei dati – confermare che le registrazioni delle transazioni e i dati finanziari restino consistenti, accurati e non corrotti tra basi di dati e sistemi integrati.
- Garanzia di sicurezza – validare che siano presenti controlli di sicurezza robusti a protezione dei dati sensibili dei clienti e degli asset finanziari da minacce informatiche, frodi e accessi non autorizzati.
- Resilienza operativa e prestazioni – valutare la stabilità e le prestazioni del sistema sotto carico elevato, validando throughput e tempi di risposta e verificando i meccanismi di failover per mantenere la continuità operativa.
- Fiducia del cliente – costruire la certezza che il prodotto funzioni in modo affidabile, tuteli gli interessi degli utenti e preservi la reputazione dell'istituto, a sostegno della fidelizzazione della clientela nel lungo periodo.

1.1.2 Tipi di Ambienti di Test Finanziari negli Istituti Finanziari

Il testing nel settore finanziario può svolgersi in diversi tipi di ambienti tecnici, a seconda dell'architettura del sistema e del dominio di business. Gli esempi seguenti illustrano categorie ricorrenti e non costituiscono un elenco esaustivo:

Ambiente omnicanale rivolto al consumatore (banca retail e commerciale). Questo ambiente privilegia un percorso del cliente unitario e continuo attraverso punti di contatto digitali e fisici integrati, tra cui applicazioni mobile, portali web, filiali, sportelli automatici (ATM) e sistemi di risposta vocale interattiva. Gli obiettivi del test riguardano la valutazione della consistenza dell'esperienza di marca, della sincronizzazione dei dati tra i canali e dell'interoperabilità tra le interfacce di front-end e i core banking system legacy.

Ambiente ad alto throughput e bassa latenza (investimenti e trading). Tipici dei motori delle borse valori e del trading algoritmico, questi ambienti devono elaborare milioni di transazioni al secondo con tempi di risposta inferiori al millisecondo. Il performance testing è la preoccupazione principale e si concentra su throughput, latenza minima e determinismo di esecuzione, per sostenere la gestione di volumi enormi a velocità costante.

Ambiente API resiliente e a logica densa (fintech).

I sistemi fintech utilizzano un'architettura a microservizi per gestire logiche di business complesse a partire da input ad alta dimensionalità. Il testing si concentra sulla resilienza operativa, assicurando che i failure restino isolati per evitare impatti a cascata sui servizi dipendenti. La validazione richiede di simulare workflow transazionali intricati, cosa ottenibile con il testing model-based, la virtualizzazione del servizio o l'orchestrazione dei test guidata dall'AI.

Ambiente di messaggistica guidata da schema (sistemi interbancari specializzati). Questo ambiente agevola la comunicazione tra banche utilizzando standard come ISO 20022 e protocolli come FIX (Financial Information Exchange). Le attività di test pongono l'accento sulla validazione dello schema per tipi di messaggia quali PAIN (avvio del pagamento), PACS (bonifici) e CAMT (gestione della liquidità).

Ambiente attuariale e dipendente dal tempo (assicurazioni e mutui). Focalizzati sul ciclo di vita di lungo periodo di polizze e finanziamenti, questi ambienti validano modelli matematici complessi per la tariffazione dei premi, la valutazione del rischio e gli ammortamenti a interesse composto. Fra gli aspetti di test principali vi sono la precisione nei calcoli multi-variabile e il **time travel testing** — una tecnica di test in cui l'orologio di sistema o il tempo simulato vengono modificati intenzionalmente per verificare il corretto comportamento delle funzionalità dipendenti dal tempo.

1.1.3 Architetture dei Sistemi Finanziari e Workflow Testabili

L'architettura di un istituto finanziario è tipicamente composta da più livelli interconnessi, ciascuno dei quali introduce aspetti di test specifici:

- **I core banking system** fungono da backend centralizzato per l'elaborazione delle transazioni finanziarie, la tenuta delle anagrafiche dei clienti e la gestione dei conti. Il testing di questi sistemi richiede di affrontare complessità architetturali specifiche, dipendenze transazionali e requisiti non-funzionali critici.
- **Il livello di integrazione e middleware** funge da infrastruttura di collegamento tra le interfacce di front-end. Il testing si concentra sulla verifica dello scambio affidabile dei dati finanziari, sul mantenimento dell'integrità dei dati tra i sottosistemi e sull'isolamento dei failure per evitare impatti a cascata sui servizi dipendenti.
- **Il front-end digitale e i canali** comprendono applicazioni mobile, portali web e terminali ATM o di punto vendita (POS). La copertura riguarda il comportamento tra dispositivi diversi, l'autenticazione biometrica, la stabilità in modalità offline e il corretto instradamento delle

transazioni; le architetture di interfaccia indipendenti dal dispositivo richiedono una resa grafica consistente su tutte le piattaforme target.

I workflow testabili in ambito finanziario comprendono:

- **Workflow transazionali.** Il testing delle transazioni finanziarie si concentra sulla verifica dell'intero ciclo di vita di un'istruzione di pagamento attraverso più sottosistemi. L'ambito comprende la correttezza delle transizioni di stato, della logica di regolamento e del comportamento di rollback, sia in condizioni di elaborazione normale sia in condizioni di failure.
- **Workflow di conformità e di identità.** L'integrità dell'onboarding del cliente si mantiene verificando i meccanismi di accertamento dell'identità, tra cui l'autenticazione dei documenti e i test biometrici, in accordo con gli standard normativi Know Your Customer (KYC). I workflow di Anti-Money Laundering (AML) vengono valutati per confermare l'individuazione accurata delle attività sospette e l'efficace screening dei soggetti rispetto alle liste di sanzioni globali, controllando al contempo il tasso di falsi positivi.
- **Workflow di investimento e di tesoreria.** Il testing dei sistemi di investimento comporta la validazione dell'intero ciclo di vita dell'operazione — dall'instradamento dell'ordine in OMS/EMS (Order Management System/Execution Management System) fino al regolamento finale — per diverse tipologie di ordine e su borse di tutto il mondo. Richiede verifiche specializzate per la logica propria di ciascun asset, come i modelli di pricing dei derivati e i “kill switch” algoritmici di controllo del rischio, oltre a un performance testing rigoroso su latenza e metriche di rischio in tempo reale.
- **Workflow operativi e di back-office.** La copertura dei workflow operativi riguarda l'integrità della riconciliazione, assicurando un flusso di dati transazionali consistente dai sistemi di front-office al libro mastro e l'allineamento con le registrazioni esterne. La copertura comprende i cicli di elaborazione periodica — come fine giornata, fine mese e fine anno — per validare l'accuratezza del regolamento, la reportistica fiscale e il mantenimento di audit trail completi a fini di governance e conformità.
- **Workflow assicurativi specializzati.** La copertura del ciclo di vita della polizza si concentra sulla correttezza delle transizioni di stato e sull'accuratezza del calcolo del premio in base alle regole di assunzione del rischio. I workflow di gestione dei sinistri sono progettati per agevolare una liquidazione sistematica, attivare i protocolli di rilevamento delle frodi ed eseguire i pagamenti. Questi processi richiedono uno scambio di dati consistente tra i sistemi assicurativi centrali per mantenere l'integrità dei dati.

1.2 Sfide e Ruolo della Conoscenza del Dominio nel Finance Testing

Nel settore dei servizi finanziari le competenze generiche di testing del software sono spesso insufficienti, a causa della complessità della base di test, della precisione richiesta nell'elaborazione delle transazioni e della severità dei vincoli normativi. La conoscenza del dominio è un fattore abilitante decisivo per mitigare le seguenti sfide di testing specifiche dei sistemi finanziari:

- **Risoluzione del problema dell'oracolo del test.** Una sfida primaria del finance testing è il problema dell'oracolo del test: determinare il risultato atteso corretto per un dato input non è banale, per via della complessità dei modelli matematici sottostanti (per es. pricing dei derivati, calcoli attuariali del rischio o curve dei rendimenti). La competenza di dominio consente di derivare in modo indipendente i risultati attesi, così da verificare la correttezza funzionale.

Syllabus-Finance Testing (CT-FT)

- Traduzione dei mandati normativi in condizioni di test. Le normative finanziarie sono spesso astratte e aperte all'interpretazione, il che rende difficile tradurle direttamente in test case eseguibili. La padronanza del dominio consente ai tester di scomporre un testo giuridico di alto livello in criteri di accettazione precisi e testabili.
- Dipendenze fra i dati. Gli input finanziari presentano dipendenze rigide fra i campi dati (per es. un determinato tipo di transazione che richiede uno specifico codice fiscale). La conoscenza del dominio consente di definire questi vincoli per generare dati di test validi, capaci di superare la logica di validazione iniziale del sistema.
- Validazione dei cicli di vita end-to-end delle transazioni. Le transazioni finanziarie attraversano spesso più sistemi eterogenei, passando dai canali di erogazione di front-office ai motori di regolamento di middle-office fino ai libri mastri di back-office. Mantenere l'integrità dei dati e la consistenza dello stato attraverso questi sistemi è una sfida primaria del testing. La competenza di dominio viene applicata per verificare il ciclo di vita completo della transazione, determinando che:
 - le transazioni siano acquisite e validate correttamente nel punto di ingresso,
 - i dati restino consistenti mentre attraversano processi quali compensazione, regolamento o conversione valutaria fra sistemi diversi,
 - lo stato finale della transazione sia riflesso accuratamente nelle registrazioni contabili, negli audit trail e nei componenti di reportistica.
- Prioritizzazione efficace nel testing basato sul rischio. A causa dei vincoli di tempo e dell'elevato volume di regression test, il testing esaustivo è impossibile. Una valutazione del rischio generica può non individuare i failure mode finanziari ad alto impatto. La competenza di dominio agevola un'analisi degli impatti accurata. I tester sanno distinguere tra difetti cosmetici e failure critici che possono causare perdite economiche, sanzioni normative o danni reputazionali.

2 Testing di Conformità – 80 minuti

Parole chiave

auditability, conformità, validazione continua automatizzata della conformità, testing di controllo, testing negativo, testing sostanziale, tracciabilità

Parole chiave specifiche del dominio

conformità normativa, General Data Protection Regulation (GDPR), Sarbanes-Oxley Act (SOX), Digital Operational Resilience Act (DORA)

Obiettivi di Apprendimento del Capitolo 2:

2.1 Obiettivi e Approcci del Testing di Conformità

FT-2.1.1 (K2) Riassumere gli obiettivi del testing di conformità e la relazione tra i suoi principali approcci del test

2.2 Le Normative Finanziarie e il Loro Impatto sul Testing

FT-2.2.1 (K2) Spiegare la rilevanza per il testing delle principali normative e standard finanziari

FT-2.2.2 (K1) Richiamare le conseguenze della non-conformità alle normative finanziarie

2.3 Caratteristiche Distintive del Finance Testing Regolamentato

FT-2.3.1 (K2) Riassumere le caratteristiche peculiari del finance testing

2.4 Auditability e Validazione Continua Automatizzata della Conformità

FT-2.4.1 (K2) Comprendere i principi fondamentali dell'auditability nel testing di conformità

FT-2.4.2 (K2) Comprendere i principi e i meccanismi di implementazione della Validazione Continua Automatizzata della Conformità (CACV) all'interno del ciclo di vita di consegna del software

Testing di Conformità

Man mano che il software diventa la spina dorsale dell'infrastruttura finanziaria globale, il punto d'incontro tra ingegneria e vigilanza giuridica si è trasformato in una frontiera operativa critica. Questo capitolo esplora il rigoroso framework del testing di conformità, una disciplina che va oltre il tradizionale rilevamento dei difetti per concentrarsi sull'integrità istituzionale e sull'aderenza alle normative. Esaminando le metodologie specializzate, i requisiti non-funzionali obbligatori e l'evoluzione verso un'auditability automatizzata e continua, si definisce come i sistemi moderni mantengano la fiducia in un contesto legislativo sempre più complesso e sottoposto a scrutinio.

2.1 Obiettivi e Approcci del Testing di Conformità

Il testing di conformità (detto anche testing di conformità normativa o regolamentare) è il processo di testing volto a determinare se un componente o un sistema è conforme a standard, leggi, normative e contratti definiti. Sebbene sia spesso classificato come testing non-funzionale, nel settore finanziario comporta spesso la validazione della logica di business funzionale e dei dati rispetto a specifici mandati normativi. Valuta se le attività, le transazioni finanziarie e le informazioni siano conformi, sotto tutti gli aspetti rilevanti, alle autorità e ai criteri che governano l'entità sottoposta ad audit.

Gli obiettivi primari del testing di conformità comprendono:

- verifica dell'aderenza – ottenere una ragionevole garanzia che il sistema e le transazioni sottostanti siano conformi ai framework normativi rilevanti e alle politiche interne,
- identificazione del rischio – individuare e valutare i rischi di non-conformità rilevante, determinando che le violazioni dei mandati legali o normativi vengano rilevate precocemente, così da mitigare potenziali sanzioni, perdite economiche o danni reputazionali,
- validazione dei controlli – valutare l'efficacia dei sistemi di controllo interno nel prevenire, rilevare e correggere i casi di non-conformità,
- produzione di evidenze – generare evidenze di audit sufficienti, pertinenti e affidabili, che dimostrino la dovuta diligenza e l'aderenza agli standard nei confronti degli stakeholder e degli organismi di regolamentazione.

Il testing di controllo e il testing sostanziale rappresentano due approcci del test complementari, utilizzati per ottenere garanzia di conformità:

- Il testing di controllo valuta se i controlli interni siano progettati in modo appropriato e operino efficacemente per prevenire, rilevare o correggere errori rilevanti o casi di non-conformità. L'obiettivo primario del testing di controllo è ottenere evidenza che i controlli operino come previsto, siano applicati in modo consistente e restino efficaci per l'intero periodo in esame. Il testing di controllo si concentra sul processo e sui meccanismi — quali workflow di approvazione, separazione dei compiti, controlli degli accessi e regole di validazione automatizzate — più che sui risultati delle singole transazioni.
- Il testing sostanziale consiste in procedure concepite per rilevare errori rilevanti o casi di non-conformità esaminando direttamente transazioni, saldi contabili e output. L'obiettivo primario del testing sostanziale è verificare l'accuratezza, la completezza e la validità dei dati e dei risultati prodotti dal sistema. A differenza del testing di controllo, che valida il modo in cui l'elaborazione viene eseguita, il testing sostanziale valida ciò che il sistema produce, indipendentemente dal fatto che i controlli siano presenti o efficaci.

2.2 Le Normative Finanziarie e il Loro Impatto sul Testing

2.2.1 Principali Normative Finanziarie e Loro Rilevanza per il Testing

Il panorama della conformità in ambito finanziario è determinato da normative, standard e linee guida a diversi livelli giurisdizionali. Alcuni sono giuridicamente vincolanti, altri orientano le best practice del settore. La loro priorità dipende dallo status giuridico e dal potenziale impatto sul business. La Tabella 1 offre una panoramica strutturata delle principali normative finanziarie e della loro rilevanza per il testing:

Tabella 1. Panoramica strutturata delle principali normative rilevanti per i sistemi finanziari e della loro rilevanza per il testing

Area di interesse	Normativa	Impatto della conformità sul testing
Protezione dei dati e privacy	General Data Protection Regulation (GDPR)	Verificare la liceità del trattamento tramite gestione del consenso, diritti dell'interessato, controlli degli accessi e privacy-by-design; utilizzare PII (Personally Identifiable Information) mascherate o sintetiche e rispettare i limiti di conservazione e di giurisdizione.
Trasparenza finanziaria	Sarbanes-Oxley Act (SOX)	Validare i controlli interni tramite separazione dei compiti, workflow di approvazione, log di audit immutabili e conservazione dello storico finanziario, utilizzando insiemi di dati anonimizzati.
Sicurezza dei pagamenti	Payment Card Industry Data Security Standard (PCI DSS)	Confermare la protezione dei dati dei titolari di carta tramite encryption, autenticazione forte e flussi transazionali sicuri, utilizzando esclusivamente Primary Account Number (PAN) tokenizzati e log mascherati.
Resilienza operativa	Digital Operational Resilience Act (DORA)	Valutare la resilienza della tecnologia dell'informazione e della comunicazione (ICT) tramite disaster recovery e pianificazione della continuità operativa (DR/BCP), failover e testing scenario-based, utilizzando insiemi di dati replicati e anonimizzati.
Pagamenti e open banking	Payment Services Directive 2 (PSD2)	Determinare la sicurezza delle operazioni di open banking testando la Strong Customer Authentication (SCA), l'autenticazione a più fattori (MFA), la sicurezza delle Application Program Interface e la gestione del ciclo di vita del consenso, utilizzando conti sintetici.
Capitale bancario e rischio	Basel III/IV	Supportare la conformità in materia di adeguatezza patrimoniale validando i modelli di rischio di credito, di mercato e di liquidità tramite stress testing e testing scenario-based, utilizzando portafogli estesi mascherati o sintetici.
Antiriciclaggio	Quinta e Sesta Direttiva antiriciclaggio dell'UE (AMLD5/AMLD6)	Verificare i controlli antiriciclaggio tramite flussi KYC, screening delle sanzioni, generazione di alert e logica di segnalazione del rischio, utilizzando pattern realistici di clienti e transazioni sintetiche.
Cripto-attività	Regolamento Markets in Crypto-Assets (MiCA)	Validare la conformità in materia di cripto-attività testando le tutele di custodia, l'integrità degli ordini e il rilevamento degli abusi di mercato, utilizzando wallet sintetici e transazioni cripto anonimizzate.

Le normative finanziarie variano da regione a regione e da giurisdizione a giurisdizione, e richiedono l'adattamento dei framework di conformità, dei meccanismi di controllo e degli standard di reportistica all'interno del processo di test.

2.2.2 Conseguenze della Non-Conformità

Il mancato rispetto dei requisiti normativi e di conformità nel settore finanziario può comportare conseguenze significative sul piano economico, legale, reputazionale e operativo:

- **Sanzioni pecuniarie e impatto economico.** Gli organismi di regolamentazione hanno il potere di comminare multe e sanzioni pecuniarie considerevoli in caso di non-conformità. Tali multe possono riguardare violazioni delle norme antiriciclaggio, delle leggi sulla data privacy o errori di segnalazione previsti dalle direttive finanziarie.
- **Sanzioni legali e normative.** La non-conformità può inoltre innescare azioni legali esecutive che vanno oltre le sanzioni pecuniarie, quali cause giudiziarie, responsabilità penale, ristrutturazione obbligatoria o nomina di un'amministrazione esterna. Nei casi più gravi le autorità di regolamentazione possono imporre misure esecutive quali la ristrutturazione obbligatoria degli asset o la nomina di un'amministrazione esterna.
- **Danno reputazionale e posizione di mercato.** Gli episodi di non-conformità possono danneggiare in modo significativo la fiducia del pubblico e degli stakeholder, con ricadute in termini di copertura mediatica negativa, preoccupazione degli investitori e abbandono da parte dei clienti.
- **Interruzione dell'operatività.** I fallimenti in materia di conformità possono determinare sospensioni del servizio, restrizioni della licenza o interventi delle autorità di regolamentazione, con conseguenti perdite di ricavi, cali di quota di mercato ed erosione della fedeltà dei clienti. Nei casi più gravi le autorità di regolamentazione possono imporre misure esecutive quali la ristrutturazione obbligatoria degli asset o la nomina di un'amministrazione esterna.
- **Rischi operativi e debito tecnico.** La non-conformità introduce rischi operativi sistemici e debito tecnico, minando la stabilità e la manutenibilità dei sistemi software. La mancata implementazione dei controlli di sicurezza prescritti espone le organizzazioni a vulnerabilità di sicurezza, tra cui violazioni dei dati e frodi.

Questi rischi sottolineano l'importanza di integrare la validazione della conformità nelle attività di sviluppo e di testing del software.

2.3 Caratteristiche Distintive del Finance Testing Regolamentato

Il testing nei sistemi finanziari regolamentati presenta caratteristiche distintive che influenzano in modo significativo il modo in cui il processo di test viene eseguito e controllato:

- **Testing guidato dal cambiamento normativo.** Il testing è spesso innescato da mandati legislativi esterni più che da obiettivi di business interni. A differenza dello sviluppo software generico, in cui i requisiti evolvono in base al riscontro del mercato, i sistemi finanziari devono adattarsi a un flusso continuo di normative nuove e aggiornate. Questo panorama normativo dinamico richiede una strategia di test caratterizzata da adattamento continuo, analisi degli impatti rigorosa e rapidità di risposta, per mantenere nel tempo la conformità giuridica.
- **L'analisi dei requisiti consapevole della normativa** è il processo specializzato di identificazione, interpretazione e mappatura dei mandati legali e di conformità in specifiche

Syllabus-Finance Testing (CT-FT)

software testabili. A differenza dell'ingegneria dei requisiti tradizionale, che si concentra sull'utilità di business, questo processo dà priorità all'aderenza alle normative esterne e alle politiche di governance interne.

- **Il testing negativo come necessità normativa.** I sistemi finanziari devono opporre resistenza attiva a usi impropri, failure e comportamenti non conformi. Il testing negativo aiuta a individuare debolezze di sicurezza, percorsi di frode e lacune logiche, sollecitando il sistema con input apparentemente validi ma vietati. In questo modo si verifica che il sistema blocchi correttamente gli accessi non autorizzati, gli sconfinamenti dei limiti e le violazioni di regole normative quali i controlli sulle sanzioni.
- **La gestione dei dati di test critica per la conformità.** Il trattamento dei dati di test è disciplinato da norme di legge che vincolano in modo sostanziale il modo in cui si esegue il testing, e che distinguono questo settore da quelli non regolamentati, dove i dati di produzione possono essere copiati a scopo di testing (vedi Capitolo 4).
- **Il testing guidato dalle evidenze** è caratterizzato dalla raccolta, dalla conservazione e dalla gestione sistematiche del testware per soddisfare auditor esterni e organismi di regolamentazione. L'obiettivo primario si sposta dal rilevamento dei difetti alla dimostrazione della dovuta diligenza e alla validazione dell'esecuzione efficace di controlli specifici.
- **Il testing non-funzionale obbligatorio** è un'attività imposta da quadri normativi, che fa della conformità una caratteristica di qualità built-in e non una preferenza di business. Aiuta a mitigare le vulnerabilità di sicurezza che potrebbero portare a frodi finanziarie o violazioni dei dati. Il testing di efficienza delle prestazioni e il testing di affidabilità sono prescritti per verificare la stabilità del sistema sotto carichi transazionali ad alta frequenza e per confermare la resilienza operativa attraverso una rigorosa validazione del disaster recovery e della continuità operativa.

2.4 Auditability e Validazione Continua Automatizzata della Conformità

2.4.1 Auditability

L'auditability, nel contesto del testing di conformità, consiste nella capacità di ricostruire, esaminare e verificare in modo indipendente le attività di test e i comportamenti del System Under Test (SUT). Comprende non soltanto la verifica funzionale del software, ma anche la documentazione rigorosa del processo di testing stesso. Tale documentazione fornisce alle autorità di regolamentazione le evidenze per verificare l'effettiva esecuzione dei controlli normativi e per confermare che il sistema operi entro i confini legali e contrattuali definiti.

I componenti principali dell'auditability sono:

- **Tracciabilità bidirezionale.** L'auditability richiede di stabilire una discendenza verificabile che colleghi i mandati normativi di alto livello agli specifici artefatti tecnici. Questo componente consente di collegare ogni requisito normativo ai test case corrispondenti (tracciabilità in avanti) e di risalire da ogni difetto o risultato del test alla regola normativa o all'obiettivo di controllo a cui si riferisce (tracciabilità all'indietro).
- **Conservazione immutabile delle evidenze.** Il testing di conformità richiede la raccolta e la conservazione sistematiche del testware. Vi rientrano test plan, requisiti approvati, log di esecuzione dettagliati e schermate dei passi critici. Questi artefatti devono essere archiviati in un formato a prova di manomissione, per fungere da evidenza inconfutabile della dovuta diligenza.

- **Integrità delle evidenze e privacy.** I sistemi devono generare audit trail sicuri e marcati temporalmente, che registrino tutte le attività degli utenti, gli eventi di accesso e gli stati delle transazioni. Questi log devono essere protetti da alterazioni non autorizzate, per poter fungere da evidenza giuridicamente valida in indagini forensi o revisioni normative. È essenziale che, nell'acquisire questi metadati, il processo incorpori tecniche di data masking per evitare che informazioni finanziarie sensibili risultino esposte nell'audit trail, sostenendo così la conformità alle normative globali sulla privacy.
- **Riproducibilità.** L'auditability richiede che i processi di test e i comportamenti del sistema siano riproducibili. Il sistema deve acquisire dati di configurazione dell'ambiente e parametri di input sufficienti a consentire a un auditor indipendente di rieseguire un test o di ripercorrere una transazione ottenendo lo stesso risultato. Questa capacità conferma che i controlli di conformità operino in modo consistente e non dipendano da variabili transitorie o non documentate.

2.4.2 Validazione Continua Automatizzata della Conformità

La Validazione Continua Automatizzata della Conformità (CACV) è la pratica di incorporare i controlli normativi e di sicurezza in forma programmatica lungo tutto il ciclo di vita di consegna del software. A differenza dei modelli di audit tradizionali, che si fondano su valutazioni periodiche riferite a un preciso istante, la CACV impiega la test automation per fornire una garanzia di conformità normativa continua e in tempo reale. Questo approccio trasforma la conformità da attività di verifica manuale e reattiva a funzionalità proattiva e built-in dell'architettura del sistema.

Meccanismi di implementazione

La CACV si fonda su implementazioni tecniche specifiche per far rispettare e monitorare i requisiti normativi:

- **Compliance as Code (CaC).** I requisiti normativi vengono tradotti in codice o script leggibili dalla macchina. Questo consente di sottoporre le regole di conformità a controllo di versione, di testarle e di eseguirle automaticamente su codice infrastrutturale e applicativo.
- **Integrazione nella pipeline e quality gate.** I controlli di conformità sono integrati direttamente nella pipeline di Continuous Integration/Continuous Deployment (CI/CD). Vengono istituiti dei "compliance gate" per bloccare automaticamente la promozione di codice non conforme verso gli ambienti di produzione.
- **Continuous Control Monitoring (CCM):** oltre alla fase di build, la CACV comporta il continuous monitoring dell'ambiente di produzione per rilevare il "drift". Il drift di configurazione si verifica quando un sistema conforme viene alterato dopo il rilascio (per es. l'apertura manuale di una porta del firewall), rendendolo non conforme.

Il workflow CACV integra la verifica normativa nel ciclo di vita di consegna del software attraverso quattro fasi iterative:

- **Elaborazione e definizione.** I framework normativi vengono analizzati per derivarne requisiti precisi e testabili, raggruppati in profili di conformità per stabilire criteri specifici per il software sottoposto a test.
- **Sviluppo.** I requisiti di conformità vengono implementati come codice eseguibile. I test case funzionali vengono sviluppati e mappati esplicitamente sulle regole normative, per stabilire una tracciabilità bidirezionale tra i requisiti e i prodotti di lavoro del test.

- **Esecuzione e ispezione automatizzate.** I test di conformità automatizzati vengono eseguiti in modo continuo all'interno della pipeline di CI/CD. I quality gate impongono l'aderenza bloccando la promozione di artefatti non conformi verso gli ambienti di produzione.
- **Valutazione e reportistica.** Gli esiti dei test vengono valutati per generare evidenze di audit immutabili e report sulle violazioni. Il continuous monitoring rileva il drift di configurazione in produzione, attivando workflow di rimedio per ripristinare la conformità.

3 Testing Basato sul Rischio – 45 minuti

Parole chiave

rischio, mitigazione del rischio, valutazione del rischio, testing basato sul rischio, matrice di tracciabilità

Parole chiave specifiche del dominio

rischio di conformità, valutazione dinamica del rischio, accettazione del rischio, evitamento del rischio, trasferimento del rischio

Obiettivi di Apprendimento del Capitolo 3:

3.1 Categorie di Rischio nei Sistemi Finanziari

FT-3.1.1 (K2) Spiegare le principali categorie di rischio nei sistemi finanziari

3.2 Principi del Testing Basato sul Rischio in Ambito Finanziario

FT-3.2.1 (K2) Spiegare i principi del testing basato sul rischio in ambito finanziario

3.3 Attività Basate sul Rischio

FT-3.3.1 (K2) Spiegare come la prioritizzazione basata sul rischio influisce sulle attività di test nelle applicazioni finanziarie

Introduzione al Testing Basato sul Rischio nei Sistemi Finanziari

Il testing basato sul rischio è un approccio strategico al testing del software che prioritizza gli sforzi di test in base ai rischi individuati per le diverse caratteristiche o funzionalità di un'applicazione software, calcolati come prodotto della probabilità di failure e del potenziale impatto sul business. Ne sono esempi il mancato rispetto di standard (per es. GDPR, PSD2, PCI DSS o MiCA) oppure calcoli o modelli di rischio difettosi. Il testing basato sul rischio è trattato nella Sezione 5 del Syllabus ISTQB Foundation Level [ISTQB_CTFL_SYL].

3.1 Categorie di Rischio nei Sistemi Finanziari

In ambito finanziario i rischi vengono individuati lungo tre dimensioni principali:

- **Rischi di business e finanziari.** Possono comprendere i rischi legati alla migrazione di dati sensibili, i difetti nel trattamento dei dati, i calcoli errati e l'applicazione errata delle regole.
- **Rischi tecnici e operativi.** Comprendono l'espansione incontrollata dell'ambito, un supporto inadeguato da parte degli strumenti oppure rischi di dipendenza più tecnici, quali l'eccessivo affidamento su strumenti specifici, framework di test automation o API.
- **Rischi normativi e di conformità.** Esistono rischi legati ai fornitori e all'esternalizzazione, come il mancato rispetto degli obblighi di conformità, di sicurezza o di prestazione da parte di fornitori di servizi terzi (aspetto particolarmente rilevante ai sensi di DORA). Possono verificarsi ritardi o fraintendimenti nell'implementazione di nuovi requisiti legali o di conformità. Questi rischi si applicano anche ai sistemi sviluppati internamente.

Il syllabus ISTQB® Foundation Level distingue tra rischi di progetto e rischi di prodotto.

I rischi di progetto riguardano la gestione e il controllo del progetto e possono influire su schedulazione, budget o ambito, compromettendo così la capacità del progetto di raggiungere i propri obiettivi.

I rischi di prodotto sono collegati alle caratteristiche di qualità del prodotto. Possono comprendere calcoli difettosi dei finanziamenti commerciali o la non-conformità ai protocolli di trasferimento elettronico di fondi applicabili. La famiglia di standard ISO 25000 definisce due modelli di qualità fondamentali: il product quality model, che valuta il software in sé (ISO/IEC 25010, 2023), e il quality-in-use model, che valuta l'effetto del software quando viene utilizzato in uno specifico contesto (ISO/IEC 25019, 2023). Qui l'attenzione è rivolta al product quality model, e la Tabella 2 illustra le nove caratteristiche di qualità e le relative sotto-caratteristiche (ISO/IEC 25010).

Tabella 2. Product quality model ISO/IEC 25010

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

Source:
ISO2500.com

Sebbene tutte e nove le caratteristiche siano essenziali, mantenere la sicurezza e preservare la privacy delle informazioni personali e finanziarie è critico in questo settore. Le violazioni dei dati possono avere impatti significativi, tra cui l'esposizione delle informazioni dei clienti agli attaccanti, il danno alla reputazione dell'azienda, ingenti perdite economiche, sanzioni legali e azioni giudiziarie. A seconda del paese, un'organizzazione può essere tenuta a farsi carico dei costi di monitoraggio del credito, a fronte dell'aumento dei tentativi di phishing e di truffa ai danni delle persone.

La cybersecurity è approfondita nei syllabus ISTQB® Security Tester [ISTQB_CT-SEC_SYL] e ISTQB® Security Test Engineer [ISTQB_CT-STE_SYL].

3.2 Principi del Testing Basato sul Rischio nei Sistemi Finanziari

Il testing basato sul rischio prioritizza le attività di test in base al livello di rischio. Nei sistemi finanziari, dove il costo dei difetti può essere estremamente elevato (per es. perdite economiche, sanzioni normative, danni reputazionali), il testing basato sul rischio è particolarmente critico. Sebbene gli istituti finanziari differiscano nella struttura, condividono funzioni simili. Occorre analizzare processi di business, transazioni finanziarie, requisiti di conformità e vulnerabilità di sicurezza. I team mirano a prioritizzare i propri test in base al rischio. Oltre a calcolare gli interessi su depositi e mutui, gli istituti finanziari svolgono molte altre funzioni, comprese quelle relative a privacy e sicurezza.

I team applicano il testing basato sul rischio prioritizzando le aree che presentano il maggior rischio di conformità o di business. Una volta individuato, ogni rischio viene valutato in termini di probabilità del rischio e impatto del rischio. Si può calcolare un valore, detto livello di rischio (per es. probabilità del rischio * impatto del rischio), per prioritizzare le aree su cui concentrare il test. I livelli di rischio possono essere espressi in forma quantitativa (per es. una probabilità di ritardo del 20%) o qualitativa (per es. basso, medio o alto).

Una matrice dei rischi (detta anche matrice probabilità-impatto) è uno strumento visuale di risk management che dispone i rischi individuati su una griglia, con la probabilità del rischio (probabilità di accadimento) su un asse e l'impatto del rischio (conseguenze in caso di accadimento) sull'altro. I rischi con probabilità e impatto più elevati ricevono la priorità di test più alta. Nella valutazione dinamica del rischio, i livelli di rischio nei sistemi finanziari evolvono man mano che vengono introdotte nuove caratteristiche, integrazioni o normative. Una rivalutazione periodica del rischio verifica che le priorità di test restino allineate alla realtà di business e normativa del momento.

Syllabus-Finance Testing (CT-FT)

Le ragioni per adottare il testing basato sul rischio comprendono:

- **allocazione efficiente delle risorse** – i team possono pianificare e destinare risorse alle aree con probabilità e impatto del rischio più elevati,
- **rilevamento precoce dei difetti** – consente ai team di individuare i difetti critici già nelle prime fasi del ciclo di vita dello sviluppo software (shift-left), offrendo l'opportunità di correggere i difetti nel codice critico già nello sprint o nell'iterazione in corso,
- **copertura ottimizzata** – il testing può essere concentrato sulle funzionalità critiche e sulle aree ad alta priorità, per determinare che gli aspetti più importanti del software siano testati in modo approfondito,
- **maggiore valore di business** – contribuisce a consegnare software che soddisfa sia i requisiti di business sia le aspettative dei clienti, aiutando ad aumentare la soddisfazione della clientela e i ricavi.

3.3 Attività di Test Relative al Testing Basato sul Rischio

Occorre considerare sia i rischi funzionali (per es. calcoli degli interessi difettosi) sia quelli non-funzionali (per es. prestazioni scadenti sotto carico elevato). Per individuare e prioritizzare i rischi è necessario coinvolgere stakeholder quali business analyst, compliance officer, team tecnico e risk manager.

Individuare quali rischi richiedono attenzione immediata e quali possono essere semplicemente monitorati aiuta i team a concentrare le risorse in modo efficace.

Prioritizzare gli sforzi di test. Esistono diverse tecniche per prioritizzare i rischi, tra cui:

- Failure Mode and Effect Analysis (FMEA) – un approccio sistematico e proattivo utilizzato per individuare, prioritizzare e mitigare i potenziali failure di una progettazione, di un processo o di un servizio prima che si verifichino.
- Fault Tree Analysis (FTA) – una tecnica di analisi dei failure deduttiva e top-down, utilizzata per individuare le root cause di un evento indesiderato a livello di sistema, mappando graficamente i failure dei componenti mediante porte logiche booleane (AND, OR).
- PRISMA (Product RiSk Management) – un approccio per individuare le aree più importanti da testare, cioè quelle che presentano il livello più alto di rischio di business o tecnico (Veenendaal, 2012).

Definire le condizioni di test. Creare condizioni di test che coprano le aree ad alto rischio individuate per verificare che la copertura sia allineata ai livelli di rischio e affronti i rischi specifici, garantendo una copertura completa e la mitigazione dei rischi individuati. Per contribuire a determinare tale completezza e conformità, si possono creare matrici di tracciabilità che collegano i rischi alle condizioni di test e le condizioni di test ai risultati del test.

Eseguire e monitorare i test. Eseguire le test suite create a partire dai test case, basati sulle condizioni di test, monitorando attentamente i risultati del test e raccogliendo i dati rilevanti.

Segnalare e mitigare i rischi. Documentare e segnalare i difetti rilevati durante il testing. Le strategie di mitigazione del rischio individuano, affrontano, riducono o gestiscono i rischi che potrebbero incidere negativamente su un progetto, su un'attività di business o su un'operazione. Le strategie di mitigazione del rischio standard sono:

- **evitamento del rischio** – intraprendere un'azione deliberata per eliminare un rischio specifico, non svolgendo l'attività che potrebbe causarlo,

Syllabus-Finance Testing (CT-FT)

- mitigazione del rischio tramite testing – ridurre la probabilità o l'impatto del rischio mediante attività di test,
- trasferimento del rischio – spostare il rischio su una terza parte, per esempio mediante un'assicurazione,
- accettazione del rischio – riconoscere e accettare il rischio.

La ISO 31000 (2018) fornisce indicazioni aggiuntive sull'integrazione del risk management nelle attività centrali e nei processi decisionali dell'organizzazione. Tali attività devono essere: integrate, strutturate e complete, personalizzate, inclusive, dinamiche, fondate sulle migliori informazioni disponibili, attente ai fattori umani e culturali, e orientate al miglioramento continuo.

4 Testing dei Dati e Gestione dei Dati – 90 minuti

Parole chiave

accuratezza dei dati, consistenza dei dati, riconciliazione dei dati, dati di test, tecnica di test

Parole chiave specifiche del dominio

audit trail, core banking system, fiducia del cliente, data privacy, profilazione dei dati, libro mastro, sistema di regolamento

Obiettivi di Apprendimento del Capitolo 4:

4.1 Accuratezza e Consistenza dei Dati

FT-4.1.1 (K2) Spiegare l'importanza dell'accuratezza e della consistenza dei dati nei sistemi finanziari

4.2 Riconciliazione dei Dati tra Sistemi Finanziari

FT-4.2.1 (K3) Applicare le tecniche di riconciliazione dei dati ai processi finanziari multi-sistema

4.3 Data Privacy e Protezione dei Dati nel Finance Testing

FT-4.3.1 (K2) Spiegare l'importanza della data privacy e della protezione dei dati nel finance testing.

Introduzione al Testing dei Dati e alla Gestione dei Dati

Nel settore finanziario la consistenza, l'accuratezza e l'integrità dei dati sono essenziali per prendere decisioni fondate e per rispettare le normative. Il testing dei dati verifica accuratezza, completezza, tempestività e discendenza dei dati finanziari lungo il loro ciclo di vita, assicurando la conformità ai framework di data governance. Gli istituti finanziari elaborano volumi enormi di dati transazionali e analitici: il testing è quindi necessario per verificare l'accuratezza e l'affidabilità delle pipeline di dati, dei report e dei modelli finanziari. Questa sezione tratta le dimensioni della qualità dei dati, le regole di validazione e tipi di test quali riconciliazione, completezza, logica di trasformazione e regression testing. Il fuoco è sul ciclo di vita dei dati finanziari, a partire dalla creazione del dato fino alla reportistica e all'individuazione di anomalie nei dati che potrebbero incidere sui livelli di rischio, sulla conformità o sulla user experience del cliente.

4.1 Accuratezza dei Dati e Consistenza dei Dati

L'accuratezza dei dati indica quanto correttamente i dati rappresentino le informazioni finanziarie reali. Dati accurati riflettono il valore effettivo di transazioni, saldi e anagrafiche dei clienti. Sono completi, aggiornati e privi di difetti che potrebbero distorcere il comportamento del sistema o i suoi output.

La consistenza dei dati indica l'uniformità della rappresentazione dei dati tra sistemi, componenti e basi di dati. Dati consistenti si presentano con lo stesso formato, valore e significato ovunque siano utilizzati, garantendo che i sistemi non forniscano informazioni contrastanti.

Importanza nei sistemi finanziari

- Reportistica finanziaria. Inesattezze o incongruenze anche minime possono propagarsi in calcoli difettosi, sintesi fuorvianti e informazioni finanziarie inaffidabili.
- Rischio e supporto alle decisioni. Le valutazioni del rischio e i modelli analitici dipendono da grandi volumi di dati storici e transazionali. Input incongruenti o difettosi possono indebolire le previsioni, distorcere i profili di rischio e ridurre la fiducia nei risultati analitici.
- Integrazione dei sistemi e automazione. Le piattaforme finanziarie sono tipicamente composte da più componenti interconnessi, tra cui i sistemi di elaborazione delle transazioni, di gestione della clientela e di riconciliazione. Dati consistenti consentono un flusso informativo fluido attraverso interfacce, livelli di integrazione e processi di trasformazione, riducendo gli interventi manuali e gli attriti operativi.

I difetti tipici di accuratezza e consistenza dei dati comprendono:

- transazioni duplicate presenti negli estratti conto,
- differenze di saldo tra i sistemi di libro mastro e di partitario,
- difformità dei dati del cliente tra i sistemi di onboarding e di gestione dell'identità,
- disallineamenti di valuta nell'elaborazione delle transazioni transfrontaliere,
- perdita o corruzione dei dati durante le attività di migrazione o di trasformazione.

Aree su cui concentrare il testing. Le attività di test si concentrano sul determinare l'accuratezza e la consistenza dei dati mentre questi si spostano, si trasformano e vengono archiviati nei diversi sistemi. Ciò comporta il confronto tra insiemi di dati di origine e di destinazione, la validazione dei risultati di riconciliazione, la conferma della logica delle regole di business e la valutazione dell'impatto delle

modifiche di sistema sui flussi dati esistenti. Comprendere le definizioni dei dati anagrafici e di riferimento è essenziale per mantenere un'interpretazione consistente dei dati tra le applicazioni.

Di seguito alcune best practice utili a sostenere l'accuratezza e la consistenza dei dati:

- applicare regole di validazione dei dati ben definite e una gestione strutturata delle eccezioni,
- utilizzare tecniche di confronto automatizzate per insiemi di dati estesi,
- eseguire la profilazione dei dati per valutare struttura, completezza e qualità,
- individuare precocemente pattern insoliti o anomalie,
- mantenere una documentazione chiara delle definizioni dei dati e dei metadati.

4.2 Riconciliazione dei Dati tra Sistemi Finanziari

La riconciliazione dei dati riguarda l'allineamento dei dati finanziari nel loro percorso attraverso più sistemi di un ecosistema finanziario. Le transazioni finanziarie attraversano tipicamente diverse piattaforme, tra cui i sistemi di elaborazione delle transazioni, i motori di regolamento, le piattaforme contabili e i livelli di reportistica. Le attività di riconciliazione sostengono la certezza che ogni sistema rifletta lo stesso esito finanziario, nonostante le differenze di logica di elaborazione, di tempistica o di trasformazione dei dati.

Quest'area è particolarmente rilevante durante le modifiche di sistema, comprese le migrazioni dei core banking system, gli aggiornamenti di piattaforma e i trasferimenti di dati su larga scala. Anche quando i sistemi funzionano correttamente sul piano tecnico, le lacune di riconciliazione possono portare a saldi difettosi, transazioni mancanti o reportistica incongruente, se i dati non sono allineati fra i sistemi.

Contesto della migrazione e della riconciliazione dei dati. Nelle iniziative di migrazione dei dati, gli istituti finanziari trasferiscono grandi volumi di dati storici e attivi, tra cui conti, saldi, transazioni e anagrafiche dei clienti. In questo contesto la riconciliazione si concentra sul confermare che i dati estratti dai sistemi legacy siano rappresentati in modo completo e corretto nell'ambiente di destinazione, dopo la trasformazione e il caricamento.

Fra le tecniche di validazione ricorrenti vi sono il campionamento dei record, il confronto di aggregati, la verifica dei checksum e la corrispondenza dei saldi tra sistema di origine e di destinazione. La riconciliazione post-migrazione confronta indicatori finanziari chiave quali saldi di apertura, totali delle transazioni e stati di registrazione, per individuare le discrepanze introdotte durante la migrazione o la trasformazione.

Riconciliazione negli ambienti finanziari integrati. Negli ambienti operativi la riconciliazione sostiene la consistenza tra sistemi interconnessi quali piattaforme di core banking, gateway di pagamento, sistemi di compensazione e regolamento e data warehouse. L'ambito va oltre i singoli record e abbraccia interi workflow di business. Per esempio, una transazione avviata da un canale di front-end dovrebbe seguire un ciclo di vita consistente — autorizzazione, regolamento, storno o rifiuto — in tutti i sistemi a valle.

Una riconciliazione efficace sostiene anche una reportistica finanziaria e operativa affidabile, verificando che le cifre aggregate siano allineate ai dati sottostanti a livello di singola transazione.

Aree principali di riconciliazione

- **Allineamento dei dati da sistema a sistema.** La riconciliazione esamina come le transazioni vengono rappresentate nel passaggio da un sistema all'altro, per esempio dalle piattaforme di elaborazione delle transazioni ai sistemi contabili e di regolamento. Stati, importi e marche temporali delle transazioni devono restare allineati attraverso le interfacce.

Syllabus-Finance Testing (CT-FT)

- **Definizione dell'ambito di riconciliazione.** Individuare con chiarezza i punti di riconciliazione — quali saldi, conteggi delle transazioni, date di registrazione e stati — verifica la copertura dei processi finanziari critici, tra cui versamenti, prelievi, bonifici e rimborsi di finanziamenti.
- **Livelli di tolleranza ed eccezioni.** Alcuni scostamenti, come le differenze di arrotondamento dovute alla conversione valutaria, possono rientrare in limiti di tolleranza predefiniti. La riconciliazione distingue gli scostamenti accettabili dalle discrepanze effettive, segnalando le eccezioni per ulteriore analisi.
- **Elaborazione batch e gestione delle scadenze di chiusura.** Molti sistemi finanziari si basano su cicli batch schedulati, in particolare nelle elaborazioni di fine giornata o di fine periodo. La riconciliazione tiene conto del trattamento delle transazioni a cavallo degli orari di cut-off (per esempio a fine mese) per verificarne la completezza ed evitare duplicazioni.
- **Riconciliazione dei libri mastri e dei saldi.** I dati a livello di transazione vengono allineati alle registrazioni del partitario e del libro mastro. Le differenze, compresi i saldi sospesi o non riconciliati, vengono tracciate fino alla loro risoluzione.
- **Frequenza della riconciliazione e gestione dei volumi.** La riconciliazione può essere eseguita in tempo reale, infragiornaliera o di fine giornata, a seconda delle esigenze di business. Il comportamento del sistema in presenza di volumi transazionali di picco viene osservato per verificare che i processi di riconciliazione restino stabili e affidabili.
- **Validazione della trasformazione e della mappatura dei dati.** I dati finanziari subiscono spesso trasformazioni quali l'applicazione di commissioni, il calcolo degli interessi e la conversione valutaria. La riconciliazione conferma che le regole di trasformazione producano esiti consistenti nei diversi sistemi.
- **Transazioni multivaluta e transfrontaliere.** Le transazioni internazionali introducono un'ulteriore complessità di riconciliazione, dovuta a tassi di cambio, valute di regolamento e differenze di tempistica. L'allineamento degli importi convertiti e dei valori di regolamento è un aspetto centrale.

Esempi di scenari di riconciliazione specifici per tipo di transazione:

- **Transazioni con carta.** I pagamenti con carta coinvolgono i sistemi emittenti, le piattaforme acquirer, i circuiti e i motori di regolamento. La riconciliazione si concentra su importi delle transazioni, commissioni, storni, chargeback e registrazioni di regolamento.
- **Transazioni ATM.** L'operatività ATM attraversa switch, processor e core banking system. La riconciliazione copre prelievi di contante, commissioni, storni, erogazioni parziali e scenari di eccezione

4.3 Data Privacy e Protezione dei Dati nel Finance Testing

I sistemi finanziari elaborano informazioni altamente sensibili, tra cui dati personali, dettagli delle transazioni e informazioni istituzionali. Durante il testing tali dati devono essere protetti da accessi, divulgazioni, alterazioni o usi impropri non autorizzati. Il testing deve inoltre confermare che il sistema tratti i dati in accordo con i requisiti applicabili di privacy e di protezione.

La data privacy riguarda la corretta raccolta, uso, archiviazione, condivisione e cancellazione delle informazioni personali e finanziarie, in linea con i requisiti legali, normativi e organizzativi.

Syllabus-Finance Testing (CT-FT)

Esempi di aree da testare in materia di privacy:

- l'accesso ai dati sensibili in base ai ruoli e alle responsabilità degli utenti
- la limitazione della visibilità dei dati sensibili in schermate, report, esportazioni e messaggi di errore
- l'uso dei dati personali solo per finalità autorizzate e in accordo con il consenso
- la corretta implementazione delle regole di conservazione e cancellazione dei dati
- la condivisione controllata dei dati attraverso interfacce e sistemi esterni
- la registrazione degli accessi e delle azioni sui dati sensibili, a supporto della responsabilità e dell'auditability

I rischi tipici per la privacy nel finance testing comprendono l'esposizione involontaria di dati personali o finanziari, la fuoriuscita di dati sensibili attraverso log o report, l'applicazione incongruente dei controlli sulla privacy e un comportamento del sistema non allineato ai requisiti di privacy.

La protezione dei dati riguarda la salvaguardia delle informazioni sensibili, soprattutto negli ambienti di test. È bene evitare i dati reali di produzione, a meno che non siano fortemente mascherati o anonimizzati sotto controlli rigorosi. Ove possibile, per il testing si dovrebbero utilizzare dati sintetici, anonimizzati, pseudonimizzati o mascherati.

Esempi di aree da testare in materia di protezione dei dati:

- la classificazione dei dati in base alla sensibilità, così da poter applicare i controlli appropriati
- il masking o l'anonimizzazione dei valori sensibili, preservando l'utilizzabilità dei dati a fini di test
- la sostituzione degli identificativi mediante pseudonimizzazione, per ridurre l'esposizione dei dati personali
- la limitazione dell'accesso al solo personale autorizzato

Syllabus-Finance Testing (CT-FT)

- la conservazione dei dati di test per il solo periodo necessario, seguita da una rimozione sicura
- la protezione dei log e degli output di monitoraggio, così che i dati confidenziali non siano visualizzati in chiaro

Il testing della privacy e della protezione dei dati nei sistemi finanziari contribuisce a ridurre i rischi di conformità, di sicurezza e operativi, sostenendo al contempo un trattamento affidabile delle informazioni sensibili.

5 Testing Funzionale e Non-Funzionale – 165 minuti

Parole chiave

disponibilità, testing back-to-back, testing dei calcoli, testing esplorativo, testing funzionale, load testing, testing non-funzionale, performance testing, testing di sicurezza, stress testing

Parole chiave specifiche del dominio

GenAI

Obiettivi di Apprendimento del Capitolo 5:

5.1 Testing Funzionale dei Sistemi Finanziari

FT-5.1.1 (K3) Applicare il testing funzionale per validare i sistemi finanziari

5.2 Rischi di Prestazione in Ambito Finanziario

FT-5.2.1 (K2) Spiegare i rischi di prestazione nei sistemi finanziari durante i periodi di picco

5.3 Performance Testing in Contesti Finanziari

FT-5.3.1 (K3) Applicare il load testing e lo stress testing in contesti specifici del settore finanziario

5.4 Testing di Sicurezza e Testing di Disponibilità

FT-5.4.1 (K2) Spiegare le esigenze di testing di sicurezza e testing di disponibilità nei sistemi finanziari

5.5 GenAI nel Finance Testing

FT-5.5.1 (K2) Spiegare come la GenAI può supportare e migliorare il finance testing

Introduzione al Testing Funzionale e Non-Funzionale

Il testing del software finanziario è cruciale per sostenere la sicurezza, la funzionalità, l'affidabilità e la conformità delle applicazioni finanziarie. Comporta tipicamente diversi tipi di testing — funzionale, di sicurezza, di prestazione e di conformità — per proteggere dai rischi e accrescere l'affidabilità del software.

5.1 Testing Funzionale dei Sistemi Finanziari

Poiché i sistemi finanziari trattano dati finanziari sensibili e transazioni monetarie reali, il costo di un failure è molto alto. Il testing richiede un approccio completo, conforme e basato sul rischio, che copra i flussi di business critici e presuppone una solida conoscenza del dominio e la consapevolezza delle normative e dei rischi.

Nel settore finanziario il testing funzionale (in particolare le tecniche di test black-box) svolge un ruolo determinante nel sostenere la correttezza funzionale e nel soddisfare i requisiti funzionali. Ciò comprende:

- verificare le funzioni finanziarie centrali, quali gestione dei conti, elaborazione delle transazioni e reportistica,
- definire l'ambito degli obiettivi funzionali e la strategia di copertura,
- effettuare la prioritizzazione basata sul rischio,
- determinare la conformità alle normative, come GDPR o PCI DSS (vedi Capitolo 2).

Diverse tecniche di test sono particolarmente rilevanti per validare le funzionalità finanziarie centrali (vedi [ISTQB_CTFL_SYL], Sezione 4.2):

- partizionamento di equivalenza – verificare la correttezza funzionale e la consistenza delle transazioni,
- analisi dei valori limite – verificare i limiti degli importi con la precisione valutaria richiesta (per es. incrementi di 0,01), compresi l'arrotondamento all'unità minima e i valori appena sotto, sul e appena sopra il limite,
- testing della tabella delle decisioni – validare i risultati del test per combinazioni di regole di business e condizioni, poiché il testing della tabella delle decisioni serve a testare le combinazioni,
- testing delle transizioni di stato – testare gli stati del conto, quali attivo/inattivo/bloccato.

La Tabella 3 riporta esempi di ulteriori tecniche di test e approcci del test adatti ai sistemi software finanziari.

Tabella 3. Esempi di tecniche di test utilizzate nel finance testing

Tecnica di test / approccio del test		Vantaggi, svantaggi e sfide
Testing dei calcoli	Questa tecnica di test comporta il ricalcolo dei valori mediante funzioni e formule note. Serve quando occorre definire formule e valori limite corretti. Ne sono esempi il calcolo dei flussi di cassa, del valore attuale netto dei flussi di cassa futuri e dei prezzi delle opzioni. La verifica tramite testing dei calcoli si concentra sull'individuazione di relazioni formalizzate tra le variabili, più che sul calcolo diretto degli output.	Vantaggi: risultati del test affidabili, facilmente formalizzabili e documentabili. Svantaggi: applicabilità limitata al testing analitico complesso, a causa degli ampi requisiti di documentazione e di implementazione. Sfide: richiede una profonda competenza di dominio.
Testing esplorativo	Questo approccio del test si concentra sull'individuazione di pattern comportamentali nei valori finanziari, senza richiedere calcoli espliciti. I test case verificano le relazioni input-output, validano le assunzioni sulle variabili, applicano valori limite (per es. il superamento del limite di importo del bonifico) e ricorrono al testing esplorativo per scoprire difetti di calcolo,	Vantaggi: esecuzione rapida, copertura ampia, basso onere organizzativo. Svantaggi: impossibilità di integrarlo in framework di automazione o in pipeline di CI/CD. Sfide: richiede qualifiche elevate e conoscenza specifica del dominio.
Testing back-to-back		Vantaggi: efficace per il regression testing. Svantaggi: la predisposizione degli ambienti di test e la sincronizzazione dei parametri di input possono risultare difficili, specialmente quando si mantengono più versioni dell'applicazione. Sfide: l'analisi delle discrepanze richiede una profonda conoscenza del dominio e la familiarità con entrambi i sistemi.

In base al tempo disponibile, alle esigenze di copertura e alle competenze del team, la scelta dell'insieme giusto di tecniche di test è determinante per ottenere risultati del test efficienti e completi. Per esempio, il testing degli ATM comprende tecniche di base (analisi dei valori limite per i trasferimenti minimi e massimi) e tecniche specializzate: testing back-to-back, testing della correttezza funzionale dei calcoli di commissioni e valute e testing esplorativo per i nuovi modelli di ATM.

Per massimizzare l'efficacia del testing funzionale, si consideri l'adozione delle seguenti best practice:

- raccogliere il riscontro effettivo degli utenti,
- utilizzare dispositivi reali – emulatori e simulatori non possono essere una soluzione di lungo periodo per il testing su dispositivo,

Syllabus-Finance Testing (CT-FT)

- testare con dati simili a quelli di produzione (per es. dati reali anonimizzati o dati di test sintetici realistici),
- coordinare e allineare gli sforzi di test tra esperti di business e tester, per raggiungere una comprensione comune e una responsabilità condivisa.

5.2 Rischi di Prestazione in Ambito Finanziario

Gli istituti finanziari dipendono da sistemi software affidabili per elaborare volumi elevati di transazioni finanziarie, erogare servizi di pagamento, gestire investimenti e rispettare i requisiti normativi. Questi sistemi devono mantenere un'efficienza delle prestazioni accettabile in condizioni operative variabili, in particolare nei periodi di picco transazionale, preservando al contempo l'integrità dei dati. I rischi di prestazione riguardano la possibilità di tempi di risposta inaccettabili, ritardi di elaborazione o degrado del throughput quando i volumi transazionali o il carico del sistema superano i livelli operativi normali.

Le sfide di prestazione ricorrenti negli istituti finanziari comprendono:

- Scalabilità – sistemi incapaci di scalare efficacemente all'aumentare del carico utente. Per esempio, un sistema di elaborazione dei pagamenti subisce failure di prestazione nei momenti di picco (festività, Natale, Black Friday, crolli di mercato).
- Difetti di concorrenza – incapacità di gestire richieste simultanee. Per esempio, dopo failure massivi, i dipendenti di una piattaforma di trading iniziano a ricaricare la pagina dell'applicazione per riprendere il servizio.
- Limitazioni infrastrutturali – hardware obsoleto o configurazioni inefficienti che ostacolano prestazioni ottimali. Per esempio, sistemi di gestione degli investimenti subiscono failure di prestazione ma non possono passare rapidamente a soluzioni esterne basate su cloud.
- Violazioni dell'integrità dei dati – perdita o corruzione dei dati transazionali sotto carico elevato. Per esempio, quando una banca predispone le segnalazioni annuali per le autorità di vigilanza, può incorrere in failure di prestazione che portano a perdita di dati e a sanzioni normative.
- Rischi da debito tecnico – la necessità di aggiornare sia il software sia i componenti hardware obsoleti, che possono guastarsi prematuramente, far crescere sensibilmente i costi di manutenzione e portare all'indisponibilità di sistemi finanziari fortemente sollecitati.
- Dipendenze da terze parti – la dipendenza da fornitori software esterni, servizi cloud e gestori di gateway di pagamento, la cui indisponibilità può ripercuotersi sulle prestazioni delle operazioni interne.

Ignorare i rischi di prestazione del software espone gli istituti finanziari a perdite economiche e a gravi danni reputazionali (per es. lamentele pubbliche dei clienti sui social media, con conseguente perdita di fiducia). Le attività per ridurre al minimo questi problemi comprendono:

- il continuous monitoring,
- i programmi di formazione del personale,
- gli audit periodici,
- le attività di test statico, che comprendono l'analisi delle metriche di carico del sistema e il loro confronto con una baseline concordata con i business analyst, per determinare se siano necessarie modifiche al profilo di carico,

- i processi di test orientati all'affidabilità, compresi performance testing e testing di disponibilità schedulati con regolarità.

5.3 Performance Testing in Contesti Finanziari

Il performance testing (per es. stress testing, load testing) ha un ruolo importante nel valutare l'affidabilità e la resilienza dei sistemi finanziari e dovrebbe essere obbligatorio negli ambienti regolamentati. La strategia di test può prevedere un ambiente separato e dedicato al load testing, che rispecchi fedelmente le caratteristiche dell'ambiente di produzione. Ciò richiede un forte isolamento e un elevato grado di somiglianza con la produzione, comprese configurazioni allineate, procedure di sincronizzazione, gestione delle dipendenze e versioni consistenti dei servizi esterni. Lo stesso vale per i dati, per la loro struttura e per la loro quantità. Il performance testing viene spesso eseguito quotidianamente. In alternativa, i team possono ricorrere al monitoraggio continuo delle prestazioni o a test di prestazione notturni. Maggiori informazioni sui concetti generali del performance testing si trovano in [ISTQB_CT-PT_SYL].

Esempi di eventi che richiedono il performance testing nei sistemi finanziari:

- il primo rilascio in produzione o una release importante (per es. l'aggiunta dell'integrazione con un servizio di monitoraggio delle frodi in un'applicazione bancaria),
- modifiche significative del sistema, quali aggiornamenti software (per es. la migrazione a una nuova versione maggiore della base di dati) o cambiamenti architetturali (per es. il passaggio da un monolite ai microservizi),
- cambiamenti attesi del profilo di carico (per es. l'apertura di nuove sedi che porta a un ampliamento della base clienti di una società di trading).

Per i sistemi finanziari ad alto carico, le attività tipiche di performance testing possono comprendere i passi seguenti:

- avvio,
- raccolta e analisi delle metriche storiche di picco volumetrico,
- predisposizione del test plan di prestazione e definizione delle metriche accettabili (SLA),
- predisposizione dell'ambiente di test, dei dati di test e degli strumenti di performance testing,
- esecuzione del performance testing,
- analisi dei risultati del test e predisposizione del test report di prestazione.

Le attività di performance testing sono trattate in dettaglio in [ISTQB_CT-PT_SYL], Capitolo 4.

I sistemi finanziari conoscono spesso volumi transazionali di picco (per es. scadenze fiscali, picchi del commercio al dettaglio, sessioni di negoziazione). Per affrontare i rischi di prestazione descritti nella Sezione 5.2, la Tabella 4 riporta esempi di ulteriori test di prestazione applicabili ai sistemi software finanziari.

Tabella 4. Ulteriori attività a supporto del testing dei sistemi software finanziari

Attività	Descrizione
Load testing	Valida la funzionalità del sistema a livelli di carico specificati, utilizzando metriche quali le transazioni al secondo.
Stress testing	Verifica il comportamento del sistema sotto carichi superiori alle condizioni normali o di picco atteso (per es. fino al 200%). Risultato atteso: il sistema può presentare prestazioni degradate o failure parziali, ma dovrebbe degradare in modo controllato (per es. restituire errori significativi anziché arrestarsi del tutto) e tornare a livelli di prestazione accettabili una volta che il carico rientra nella norma. Metriche: latenza delle richieste, tasso di errore, throughput e utilizzo delle risorse (CPU, memoria) durante e dopo il periodo di stress.
Endurance	Determina se il SUT operi in modo stabile sotto carico prolungato nel tempo. Il monitoraggio di metriche quali l'utilizzo dell'unità centrale di elaborazione (CPU) e delle risorse può aiutare a rilevare un degrado (per es. perdite di memoria). Ciò si applica al testing di endurance.
Disponibilità dei sistemi esterni	Misura prestazioni e stabilità del sistema (tempi di risposta, tassi di errore, consumo di risorse) quando i sistemi esterni da cui dipende sono lenti, vanno in timeout o non sono disponibili. Aiuta ad assicurare che la logica di gestione dei failure (circuit breaker, ritentativi) non introduca degrado delle prestazioni o perdite di risorse. Metriche: utilizzo di CPU e memoria, percentili di latenza delle richieste, numero di eccezioni di timeout.
Failover	Verifica la stabilità del sistema al riavvio, la resistenza ai crash, la velocità di ripristino e il back-up. I sistemi basati su cloud possono eliminare pod durante il testing. Applicabile allo spike testing, che determina la resilienza del sistema a improvvisi picchi del carico di punta e il ritorno a un funzionamento stabile.
Disponibilità dei data center	Verifica il corretto bilanciamento delle richieste tra i data center durante i periodi di indisponibilità, usando metriche quali il tasso di failure, le transazioni e le richieste HTTP al secondo. Utile per il testing di scalabilità, lo spike testing e lo stress testing.

Adottando procedure regolari di performance testing e investendo in un'infrastruttura affidabile, gli istituti finanziari possono ridurre il rischio di costose interruzioni di servizio.

5.4 Testing di Sicurezza e Testing di Disponibilità

Il testing di sicurezza del software finanziario verifica che il sistema protegga la confidenzialità, l'integrità e la disponibilità dei dati, contribuendo così a prevenire frodi e perdite economiche. Queste attività dovrebbero essere integrate lungo tutto il ciclo di vita dello sviluppo, per esempio individuando precocemente le lacune rispetto agli standard e applicando il threat modelling per mitigare i rischi finanziari, oppure conducendo review di sicurezza specialistiche su progettazioni e architetture.

I tipi di test di sicurezza comprendono:

Syllabus-Finance Testing (CT-FT)

- lo scanning delle vulnerabilità,
- il penetration testing,
- lo Static/Dynamic Application Security Testing (SAST/DAST),
- l'analisi delle dipendenze e dei componenti di terze parti.

Le aree principali del finance testing comprendono:

- il testing delle configurazioni cloud e della gestione dei segreti ai fini della conformità (per es. per l'elaborazione dei pagamenti),
- il testing degli algoritmi di encryption dei dati (per es. nei settori contabile e bancario),
- la validazione dell'autenticazione a più fattori, dei controlli di accesso basati sui ruoli e dei cicli di vita dei token, e la determinazione che il traffico delle API sia instradato in modo sicuro attraverso gateway dedicati (per es. applicazioni mobile e di web banking),
- la verifica dell'integrità dei log di sicurezza, della loro configurazione, delle procedure di gestione e dei meccanismi di allerta (per es. a tutela delle informazioni personali degli assicurati nel settore assicurativo).

Fra le best practice per eseguire il testing di sicurezza:

- utilizzare strumenti specializzati,
- seguire gli standard applicabili (per es. OWASP),
- integrare la sicurezza nel processo di sviluppo (DevSecOps),
- incorporare il threat modelling,
- gestire i rischi legati alle terze parti e alla catena di fornitura,
- progettare ambienti di test sicuri e trattare i dati di test in modo responsabile,
- allinearsi al testing di conformità (vedi Capitolo 2).

Per maggiori informazioni si veda [ISTQB_CT-SEC_SYL].

Il testing di disponibilità determina se il funzionamento sia continuo durante i carichi di picco, così da prevenire perdite di transazioni, impatti sui ricavi e perdita della fiducia del cliente. Gli obiettivi principali e le metriche correlate comprendono:

- obiettivi di ripristino: Recovery Time Objective (RTO) per i servizi IT e Recovery Point Objective (RPO) per le transazioni chiave,
- prestazioni sotto carico: tempo di esecuzione, tempo di risposta e throughput per le transazioni chiave,
- affidabilità del sistema: tasso di failure, Mean Time Between Failures (MTBF), Mean Time to Failure (MTTF) e disponibilità,
- validazione della resilienza: bilanciamento del carico, test di failover e Mean Time to Repair (MTTR).

Le strategie di test per mitigare le sfide di disponibilità comprendono:

Syllabus-Finance Testing (CT-FT)

- scalabilità: eseguire load testing e stress testing con scenari di ora di punta e validare il comportamento di scalabilità automatica,
- infrastruttura: condurre un testing di failover sistematico per verificare il comportamento di ripristino e la continuità,

Il testing di sicurezza e il testing di disponibilità sono essenziali per sistemi software finanziari affidabili. Il testing di sicurezza protegge dagli attacchi malevoli, mentre il testing di disponibilità verifica la continuità del servizio e il ripristino in condizioni avverse. Insieme, queste attività contribuiscono all'affidabilità e alla resilienza complessive del sistema.

5.5 GenAI nel Testing del Software Finanziario

L'integrazione della Generative Artificial Intelligence (GenAI) nel testing dei sistemi finanziari può migliorare efficienza e consistenza in un ambiente fortemente regolamentato. Applicando tecniche di prompt engineering, la GenAI può supportare le attività di test lungo tutto il processo di test, comprese analisi dei test, progettazione dei test, implementazione dei test, monitoraggio dei test e controllo dei test, e completamento dei test.

Le organizzazioni finanziarie possono adottare nel proprio ciclo di vita dello sviluppo software gli assistenti AI di uso comune elencati nella Tabella 5.

Tabella 5. Assistenti AI di uso comune applicabili al finance testing

Attività di test	Aspetto assistenziale dell'AI
Testing in fase di sviluppo	Gli assistenti AI integrati possono aiutare gli sviluppatori a generare test di unità e a risolvere automaticamente difetti minori, utilizzando modelli calibrati sugli standard di codifica e sui pattern consolidati dell'organizzazione.
Analisi dei test	L'assistente AI supporta i tester analizzando le API e proponendo requisiti e condizioni di test da sottoporre a review e affinamento.
Progettazione e implementazione dei test	L'assistente AI: - costruisce e sincronizza modelli di test a partire dal codice, genera test case all'interno degli ambienti di sviluppo e carica i risultati del test negli strumenti di test management, - crea e sottopone a review test automatizzati a partire dai test case esistenti, e genera test case di interfaccia utente e di API a partire dai requisiti, - verifica che i test case non violino i requisiti di information security, - abilita la test automation low-code/no-code, aiutando i tester a creare script di test automatizzati assistiti dall'AI mediante interfacce visuali e componenti predefiniti, riducendo lo sforzo di codifica manuale.
Monitoraggio dei test e controllo dei test	L'assistente AI analizza i log di test per rilevare anomalie e individuare difetti durante il testing.
Completamento dei test	L'assistente AI supporta la creazione e la validazione dei test report e dei defect report.

La GenAI può potenziare il testing del software finanziario, ma introduce anche delle sfide, in particolare la disponibilità limitata e il costo elevato di dati etichettati di alta qualità. Per massimizzare il valore della

GenAI, gli istituti finanziari dovrebbero dare priorità all'integrità dei dati, all'aderenza alle normative, allo sviluppo delle competenze e al miglioramento dell'infrastruttura. I rischi economici andrebbero gestiti tramite iniziative pilota e una pianificazione realistica. Il successo andrebbe misurato con metriche chiare (per es. il tempo di ciclo di test e i tassi di difettosità) e valutando opportunità quali la generazione autonoma dei test e il monitoraggio continuo della conformità. I ruoli di Quality Control si estenderanno probabilmente fino a comprendere la mitigazione proattiva del rischio, l'apprendimento continuo, la supervisione dell'addestramento dei modelli AI, l'adozione di best practice e l'allineamento agli obiettivi di business. Le competenze di analisi avanzata e di debugging dell'AI diventeranno sempre più importanti.

6 Test Automation – 105 minuti

Parole chiave

test automation

Parole chiave specifiche del dominio

DTO, privacy

Obiettivi di Apprendimento del Capitolo 6:

6.1 Ruolo della Test Automation nel Finance Testing

FT-6.1.1 (K2) Spiegare come la test automation supporta l'efficienza dei test in ambito finanziario

6.2 Strategie di Test Automation

FT-6.2.1 (K3) Applicare le strategie di test automation in panorami IT finanziari legacy e moderni

6.3 Sfide della Test Automation in Ambienti Regolamentati

FT-6.3.1 (K2) Spiegare le sfide della test automation in ambienti regolamentati

6.4 Sfide nei Diversi Tipi di Test Automation

FT-6.4.1 (K2) Spiegare le sfide della test automation su componenti mobile, frontend e backend

Introduzione alla Test Automation

La test automation ha un ruolo importante nel migliorare la stabilità e l'efficienza del testing dei sistemi finanziari. Nel settore finanziario, dove precisione e rapidità sono essenziali (per es. calcolare l'interesse composto, verificare i punteggi di credito o eseguire ampie test suite di regressione), l'automazione offre vantaggi significativi rispetto al testing manuale. Utilizzando strumenti e framework specializzati, i test engineer possono validare in modo efficiente calcoli complessi, simulare volumi transazionali elevati e verificare la conformità ai requisiti normativi. Per ulteriori informazioni si rimanda a [ISTQB_CTAL-TAE_SYL].

6.1 Ruolo della Test Automation nel Finance Testing

La test automation offre benefici significativi per il testing dei sistemi finanziari, quali cicli di test più brevi, maggiore accuratezza e migliore scalabilità. Per esempio:

- L'automazione consente un'esecuzione dei test consistente e fornisce risultati del test precisi, riducendo al minimo le discrepanze dovute a errori di immissione manuale.
- L'automazione supporta un regression testing rapido dopo gli aggiornamenti (per es. delle funzioni di credito o di pagamento), liberando i tester manuali così che possano concentrarsi su scenari complessi.
- Gli script di test automatizzati possono essere schedulati per esecuzioni frequenti, allineate ai rilasci, fornendo un riscontro rapido e sostenendo una consegna iterativa.
- I test automatizzati possono simulare scenari di carico di punta ed essere eseguiti in modo consistente su più ambienti con configurazioni allineate.
- Maggiore conformità e sicurezza – la test automation può verificare sistematicamente la conformità agli standard (per es. PCI DSS per i pagamenti con carta e i controlli AML/CFT) e generare evidenze verificabili in sede di audit. I test automatizzati possono inoltre essere eseguiti in ambienti ad accesso limitato senza concedere accessi manuali, facendo girare script di test ripetibili attraverso pipeline controllate.
- I processi automatizzati possono creare dati di test end-to-end complessi (per es. clienti con storico creditizio, fatture, carte e modelli di transazione).

Nonostante i suoi vantaggi, l'implementazione della test automation presenta ostacoli peculiari del dominio finanziario:

- **Complessità** – i sistemi finanziari comportano spesso workflow complessi, che richiedono algoritmi avanzati per simulare accuratamente gli scenari reali. Per esempio, automatizzare i test di un processo di stipula di un mutuo può richiedere la copertura di scoring, verifica del reddito, calcolo delle rate e integrazioni con registri esterni.
- **Costo** – lo sforzo e la spesa iniziali per progettare, implementare e mantenere una test automation efficace possono essere considerevoli. Nei sistemi finanziari il ritorno sull'investimento deriva spesso meno dalla riduzione del testing manuale e più dalla riduzione della probabilità e dell'impatto del rischio di failure costosi, quali interruzioni di servizio, transazioni fallite e sanzioni normative.

Syllabus-Finance Testing (CT-FT)

- **Carenza di competenze** – la mancanza di professionisti che padroneggino sia la logica di business finanziaria sia le competenze tecniche di test automation richieste può limitare l'adozione e la scalabilità delle iniziative di test automation.

Affrontare questi aspetti richiede:

- pianificazione strategica,
- investimenti in programmi di formazione (matrici delle competenze, piani di sviluppo individuali e mentoring),
- framework e strumenti di test standardizzati (per es. per simulare API esterne)
- integrazione della test automation nel ciclo di vita dello sviluppo tramite pipeline di CI/CD,
- collaborazione fra gli stakeholder a tutti i livelli di test; questi elementi dovrebbero essere riflessi nella strategia di test automation.

6.2 Strategie di Test Automation

La test automation offre vantaggi significativi, tra cui risparmi di tempo e di costi. Progettare e implementare una strategia di test automation ottimale richiede però una pianificazione accurata e la considerazione di diversi fattori. Le strategie di test automation ricorrenti comprendono:

- I diversi schemi di distribuzione dei test (piramide, cono gelato, clessidra, ombrello) orientano i livelli della test automation, aiutando a valutare la situazione attuale e a fissare obiettivi di miglioramento. I sistemi legacy richiedono strategie diverse rispetto alle nuove implementazioni.
- Lo shift-left dà priorità alla test automation precoce e alla conformità nelle pipeline di sviluppo, mentre lo shift right monitora in tempo reale la qualità, l'integrità delle transazioni e il rilevamento delle frodi negli ambienti di produzione.
- In un'organizzazione finanziaria con un panorama infrastrutturale complesso (per es. un sistema di elaborazione legacy integrato con una moderna applicazione di pagamento mobile), si utilizzano approcci del test differenti a seconda del modello di ciclo di vita dello sviluppo software, quali:
 - le pratiche di sviluppo software Agile, con enfasi sulla test automation,
 - i modelli di ciclo di vita dello sviluppo software legacy (per es. lo sviluppo software sequenziale), in cui il testing è spesso pianificato ed eseguito in fasi distinte,
 - le pratiche DevOps, che abilitano il continuous testing attraverso pipeline di CI/CD.

Per esempio, privilegiando inizialmente la test automation su tutti i livelli della piramide di test – per es. test di componente, test di API e di servizio e test di interfaccia utente – una banca può liberare capacità di testing da dedicare alla validazione su dispositivi reali quali ATM e terminali POS, costosi e difficili da automatizzare. In questo esempio la banca mette in atto un insieme di approcci del test: adotta uno schema di distribuzione dei test, si concentra sulla test automation e dà priorità alla test automation precoce.

Per ulteriori informazioni sugli approcci del test ricorrenti nella definizione di una strategia di test automation si rimanda a [ISTQB_CT-TAS_SYL], sezione 3.1.1.

Syllabus-Finance Testing (CT-FT)

Oltre agli approcci comuni, occorre tenere conto delle specificità proprie del settore finanziario. Nel pianificare una strategia di test automation per il settore finanziario è importante considerare i fattori seguenti, che possono influenzare le decisioni:

- **Elevate esigenze di accuratezza** – i difetti nei calcoli finanziari possono avere conseguenze gravi. Per esempio, i sistemi finanziari possono memorizzare i valori monetari con tipi di dato differenti ed eseguire i calcoli con livelli di precisione diversi. Nel definire la strategia di test è importante tenere conto di queste differenze e verificare che i test applichino criteri di precisione e di verifica più stringenti di quanto sarebbe tipicamente richiesto in domini non finanziari.
- **L'implementazione di test automatizzati end-to-end su più sistemi finanziari interconnessi** introduce una notevole complessità tecnica, in particolare in ambiti quali i sistemi contabili con workflow di fatturazione complessi.
- **Uso di dati in tempo reale (o quanto più possibile vicini al tempo reale) negli script di test automatizzati** – la struttura e il contenuto dei dati di ingresso possono cambiare nel tempo. Per esempio, i pattern di transazione dei clienti possono variare con la stagione e con l'offerta di prodotti. I test automatizzati dovrebbero rispecchiare il più fedelmente possibile gli scenari reali, utilizzando dati di pre-produzione anonimizzati o dati di test aggiornati con regolarità.
- **Oracolo del test (o pseudo-oracolo) automatizzato** – nello sviluppo di un nuovo sistema, i risultati del test possono essere confrontati con un'applicazione di riferimento. Questo approccio può avere dei limiti, perché mantenere allineati i due sistemi è difficile e le differenze nelle regole di business o nel trattamento dei dati possono incidere sui risultati del test.
- **Approccio al regression testing automatizzato** – confrontare i calcoli dell'applicazione corrente con quelli delle versioni precedenti o con risultati del test di riferimento per verificarne la correttezza, tenendo conto dei costi di manutenzione di due ambienti di test.

6.3 Sfide della Test Automation in Ambienti Regolamentati

Le organizzazioni che operano in ambito finanziario devono rispettare molteplici insiemi di regole, nazionali e internazionali, quali GDPR, SOX, PCI DSS e DORA. Queste regole impongono ulteriori sfide di cui tenere conto nella pianificazione di una strategia di test automation:

- **Complessità delle normative** – le normative introducono complessità imponendo requisiti stringenti di protezione dei dati, di privacy e di sicurezza, che incidono sulla progettazione della test automation. Un esempio è l'aderenza agli standard PCI DSS nel testing delle transazioni ATM.
- **Problemi di manutenzione** – sostenere la test automation comporta attività ricorrenti quali la modifica del codice applicativo, la gestione di script e librerie di test, l'aggiornamento delle integrazioni esterne e l'adeguamento delle test suite.
- **Logging e dimostrabilità** – i log delle transazioni di business devono essere mantenuti e conservati, insieme ai log di test, per la validazione da parte degli auditor. Le autorità di regolamentazione esigono la prova dell'efficacia del testing e la riproducibilità dei percorsi delle transazioni ai fini delle indagini.
- **Strumenti di test automatizzato specifici** – le organizzazioni finanziarie ricorrono spesso a strumenti di test automation proprietari, calibrati sulle proprie esigenze peculiari. Questi strumenti non hanno un'ampia diffusione di mercato né un supporto centralizzato: è il caso, per esempio, degli strumenti di test per il testing biometrico e per POS e ATM.

Syllabus-Finance Testing (CT-FT)

Le attività per superare queste sfide comprendono:

- Complessità delle normative
 - Creare una mappa del testing per la complessità delle normative, cioè una tabella in cui, per ciascun requisito normativo, siano definiti l'area di impatto, i requisiti sui dati di test e le condizioni di test critiche.
 - Anonimizzazione dei dati (masking). Modificare i dati reali rimuovendo o offuscando gli identificativi personali, così che i dati restino strutturalmente integri e realistici ai fini del testing ma non siano più considerati dati personali ai sensi di normative quali il GDPR.
 - Generazione di dati di test sintetici. Creare insiemi di dati artificiali che riproducano le caratteristiche del mondo reale, assicurando che siano liberi da qualsiasi vincolo normativo.
- Problemi di manutenzione
 - Utilizzare un data transfer object (DTO) comune, se previsto dal contratto di interazione.
 - All'interno del framework di test automation dovrebbe essere implementato l'isolamento della logica di test dalle risorse (dettagli di interfaccia utente, dati di test).
 - Implementare l'avvio automatico degli script di test automatizzati a ogni modifica del codice, per individuare rapidamente i difetti.
- Logging e dimostrabilità
 - Implementare il logging end-to-end dei test. Ogni test run dovrebbe generare automaticamente un testware dettagliato e strutturato.
 - Automatizzare la reportistica di audit. Sviluppare report automatizzati che dimostrino la copertura delle funzioni critiche per la conformità, la loro storia di esecuzione e la prova dell'esecuzione prima del rilascio.
- Strumenti di test automatizzato specifici
 - Collocare il codice sorgente degli strumenti interni in repository interni condivisi, accessibili a tutta l'organizzazione (inner source).
 - Nello sviluppo degli strumenti interni occorre considerare la possibilità di integrarli mediante protocolli standard (REST API).

6.4 Sfide nei Diversi Tipi di Test Automation

Con l'aumentare della complessità dei sistemi finanziari, dovuto ai progressi di tecnologie quali cloud computing, architetture orientate ai servizi, AI e piattaforme mobile, gli approcci del test manuali incontrano numerose difficoltà. Dalle app di mobile banking ai sistemi finanziari in cloud, queste applicazioni richiedono un testing rigoroso per determinarne affidabilità, sicurezza e conformità normativa. La test automation può rendere più snello questo processo, ma presenta anch'essa delle sfide, in particolare nel testing dei componenti mobile, di front-end e di back-end.

Pur portando notevoli vantaggi, la test automation lascia aperte alcune sfide:

- **Automatizzare le applicazioni mobile** – nel settore finanziario è importante considerare gli aspetti di sicurezza e conformità, l'usabilità e la user experience, compresi la variabilità delle

Syllabus-Finance Testing (CT-FT)

condizioni di rete, l'ottimizzazione della durata della batteria, la device fragmentation e le sfide specifiche di conformità legate alla sicurezza o all'encryption.

- **Automatizzare le applicazioni web di frontend** – ci si concentra sul determinare usabilità, accessibilità e conformità nelle applicazioni finanziarie, compresi la compatibilità cross-browser, la gestione dei contenuti dinamici, i limiti e l'instabilità dell'automazione della GUI e la test automation con browser headless.
- **Automatizzare il backend** – ci si concentra sull'integrità dei dati, sull'integrazione e sulla logica di business nei sistemi finanziari, compresi la complessità dell'integrazione fra API, la garanzia dell'integrità dei dati e i difetti di bilanciamento del carico e di scalabilità.
- **Testing di sicurezza automatizzato** – nel settore finanziario riguarda:
 - il masking obbligatorio dei dati sensibili,
 - l'elevato numero di risultati del test falsi positivi e falsi negativi, e la conseguente necessità di una verifica manuale periodica dei risultati del test degli strumenti di sicurezza,
 - il lavoro con traffico cifrato e autenticazione.

La test automation apporta benefici enormi allo sviluppo del software finanziario, ma comporta sfide significative legate ai componenti mobile, di frontend e di backend.

Le attività per superare queste sfide comprendono:

- adottare una piramide di test basata sul rischio,
- gestire i dati di test e isolare gli ambienti nella CI/CD,
- ridurre l'instabilità con locator affidabili, attese esplicite e setup/teardown idempotenti,
- definire una matrice dispositivi/rete, sfruttare i device cloud e preferire i framework di piattaforma per garantire stabilità — aspetto applicabile al testing su mobile.

La test automation nel software finanziario ha grandi potenzialità di migliorare l'efficienza e di sostenere la qualità dei servizi finanziari. La GenAI si annuncia promettente per la test automation in ambito finanziario, offrendo copertura dei test completa, rilevamento dei difetti, automazione delle attività e riscontro rapido. Per realizzare questo potenziale occorre superare le sfide delineate.

7 Elenco delle Abbreviazioni

Abbreviazione	Definizione
AML	Anti-Money Laundering
Basel III / IV	Insieme di misure concordate a livello internazionale dal Comitato di Basilea per la vigilanza bancaria
CAC	Continuous Automated Compliance
CACV	Continuous Automated Compliance Validation
CAMT	Cash Management (categoria di messaggi ISO 20022)
CCM	Continuous Compliance Management
CFT	Combating the Financing of Terrorism
CTFL	Certified Tester - Foundation Level
CT-FT	Certified Tester - Finance Testing
CPU	Central Processing Unit
DAST	Dynamic Application Security Testing
DORA	Digital Operational Resilience Act
DTO	Data Transfer Object
EMS	Execution Management System
GDPR	General Data Protection Regulation
GenAI	Generative Artificial Intelligence
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
KYC	Know Your Customer (or Client)
MiCA	Markets in Crypto-Assets Regulation
MFA	Multi-Factor Authentication
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
OMS	Order Management System
OWASP	Open Worldwide Application Security Project
PACS	Payments Clearing and Settlement (categoria di messaggi ISO 20022)
PAIN	Payment Initiation (categoria di messaggi ISO 20022)
PAN	Device Primary Account Number
PCI DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
POS	Point of Sale
PSD2	European Union's Revised Payment Services Directive 2

Syllabus-Finance Testing (CT-FT)

RTO	Recovery Time Objective
RPO	Recovery Point Objective
SAST	Static Application Security Testing
SCA	Strong Customer Authentication
SOX	Sarbanes-Oxley Act
SUT	System Under Test

8 Termini Specifici del Dominio non Relativi al Testing

Termine	Definizione
accuratezza dei dati	Misura di quanto fedelmente le informazioni rappresentano gli oggetti o gli eventi registrati.
audit trail	Sistema che tiene traccia delle transazioni di dettaglio relative a qualsiasi voce di una registrazione contabile.
Basel III / IV	Framework normativo internazionale per le banche che rafforza i requisiti patrimoniali, irrigidisce le regole su rischio e liquidità ed esige una reportistica accurata e verificabile in sede di audit.
conformità normativa	Il processo con cui un'organizzazione rispetta leggi, normative, standard e regole applicabili, stabiliti da governi e organismi di regolamentazione, a sostegno di un'operatività legale, etica e sicura.
consistenza dei dati	Accuratezza, completezza e correttezza dei dati archiviati in una base di dati
data privacy	La data privacy è la protezione delle informazioni personali da accessi, divulgazioni, alterazioni o distruzioni non autorizzati. Comprende le politiche, le procedure e le tecnologie che disciplinano il modo in cui i dati privati delle persone sono raccolti, archiviati, trattati e condivisi dalle organizzazioni.
Data Transfer Object (DTO)	Pattern di progettazione utilizzato nello sviluppo software per trasferire in modo efficiente i dati tra livelli o componenti diversi di un'applicazione. Contiene tipicamente i soli campi necessari al trasferimento delle informazioni, senza logica di business né comportamento, così da garantire la separazione delle responsabilità e migliorare le prestazioni riducendo al minimo il traffico di rete.
Digital Operational Resilience Act (DORA)	Regolamento che rafforza la resilienza operativa della tecnologia dell'informazione e della comunicazione (ICT) e dei fornitori terzi nel settore finanziario dell'UE.
fiducia del cliente	La fiducia che un consumatore ripone in un'azienda quanto alla capacità di tenere fede ai propri impegni e di mantenere le proprie promesse.
GenAI	La Generative Artificial Intelligence (GenAI) è una branca dell'Artificial Intelligence che utilizza modelli estesi e pre-addestrati per generare output simili a quelli umani, quali testi, immagini o codice. I large language model (LLM) sono modelli di GenAI pre-addestrati su ampi insiemi di dati testuali, il che consente loro di determinare il contesto e di produrre risposte pertinenti ai prompt dell'utente.
General Data Protection Regulation (GDPR)	Regolamento dell'Unione Europea (UE) che stabilisce regole complete in materia di data privacy e di protezione dei dati personali dei residenti.

Syllabus-Finance Testing (CT-FT)

istituto finanziario	Azienda o organizzazione che svolge transazioni finanziarie e monetarie, agendo da intermediario per fornire servizi finanziari quali finanziamenti, depositi, investimenti e assicurazioni a persone, imprese e amministrazioni pubbliche.
Know Your Customer (KYC)	Processo obbligatorio con cui gli istituti finanziari verificano l'identità dei propri clienti e ne valutano i rischi potenziali.
libro mastro	Il sistema contabile centrale e primario di un'azienda, utilizzato per registrare tutte le sue transazioni finanziarie sui diversi conti, quali attività, passività, patrimonio netto, ricavi e costi.
Open Worldwide Application Security Project (OWASP)	Fondazione senza scopo di lucro che opera per migliorare la sicurezza del software.
Payment Card Industry Data Security Standard (PCI DSS)	Insieme di standard di sicurezza che ogni impresa che tratta dati di carte di credito o di debito deve rispettare per prevenire le frodi.
privacy	Il diritto di controllare le proprie informazioni personali, il proprio spazio e le proprie comunicazioni, al riparo da intrusioni e osservazioni non autorizzate.
profilazione dei dati	Analisi, esame e sintesi sistematici di insiemi di dati, allo scopo di comprenderne struttura, contenuto, relazioni e qualità.
PSD2	Payment Services Directive 2. Direttiva dell'UE che regola i servizi di pagamento per accrescere la concorrenza, migliorare la sicurezza e aprire il mercato a nuove imprese, dette fornitori terzi.
riconciliazione dei dati	Processo sistematico di confronto dei dati provenienti da fonti diverse, allo scopo di determinarne accuratezza, consistenza e completezza.
rischio di conformità	Il rischio di sanzioni legali, perdite economiche o danni reputazionali che un istituto può subire a seguito del mancato rispetto di leggi, normative, codici di condotta e standard di best practice.
Sarbanes-Oxley Act (SOX)	Legge federale degli Stati Uniti che impone alle società quotate di istituire e mantenere registrazioni contabili accurate e controlli interni solidi, per prevenire le frodi societarie e tutelare gli investitori.
sistema di regolamento	Insieme di processi, regole e infrastrutture che consente il trasferimento definitivo di denaro o di titoli per adempiere a un'obbligazione finanziaria fra le parti.
standard normativo	Regola o requisito ufficiale stabilito da un governo o da un'altra autorità per determinare i livelli minimi di qualità, sicurezza o prestazione in un settore o in un processo.
trasferimento del rischio	
valutazione periodica del rischio	Esame schedulato e ricorrente delle operazioni, dei sistemi o dei progetti di un'organizzazione, allo scopo di individuare, analizzare e mitigare le minacce in evoluzione.

Syllabus-Finance Testing (CT-FT)

violazione dei dati	Incidente di sicurezza in cui informazioni confidenziali o sensibili vengono illecitamente consultate, visualizzate, divulgate, copiate o sottratte da una persona o da un gruppo non autorizzato, compromettendone sicurezza, integrità o confidenzialità.
---------------------	---

9 Riferimenti

9.1 Standard

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>

ISO 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 Documenti ISTQB®

[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>

Syllabus-Finance Testing (CT-FT)

[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 Riferimenti al Glossario

- Agile Alliance <https://www.agilealliance.org/agile-practice-guide/>
- IREB-CPRE for Requirements Engineering <https://www.ireb.org/en/cpre/glossary>
- Glossario ISTQB® <https://glossary.istqb.org/>

9.4 Libri, Articoli e Pagine Web

Libri

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>

Pagine web

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

Hayes (2025) Adam Hayes, "What Is a Financial Institution", da <https://www.investopedia.com/terms/f/financialinstitution.asp>

Joseph (2020) Timothy Joseph. "Financial Domain Testing: The Breakdown", da <https://blog.qasource.com/financial-domain-testing-the-breakdown/>

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

I riferimenti precedenti rimandano a informazioni disponibili su Internet e altrove. Sebbene tali riferimenti

Syllabus-Finance Testing (CT-FT)

siano stati verificati al momento della pubblicazione del presente syllabus, ISTQB® non può essere ritenuto responsabile qualora i riferimenti non fossero più disponibili.

Appendice A – Obiettivi di Apprendimento/Livello Cognitivo di Conoscenza

Gli obiettivi di apprendimento specifici che si applicano a questo syllabus sono indicati all'inizio di ogni capitolo. Ogni argomento del syllabus sarà esaminato in base al suo obiettivo di apprendimento.

Gli obiettivi di apprendimento iniziano con un verbo di azione corrispondente al livello cognitivo di conoscenza, come elencato di seguito.

Livello 1: Ricordare (K1)

Il candidato è in grado di ricordare, riconoscere e richiamare un termine o un concetto.

Verbi di azione: richiamare, riconoscere.

Esempi
Richiamare i concetti della piramide di test.
Riconoscere gli obiettivi tipici del testing.

Livello 2: Comprendere (K2)

Il candidato è in grado di selezionare le ragioni o le spiegazioni delle affermazioni relative all'argomento, ed è in grado di riassumere, confrontare, classificare e fornire esempi per il concetto di testing.

Verbi di azione: classificare, confrontare, differenziare, distinguere, spiegare, fornire esempi, interpretare, riassumere

Esempi	Note
Classificare gli strumenti di test in base al loro scopo e alle attività di test che supportano.	
Confrontare i diversi livelli di test.	Può essere usato per cercare somiglianze, differenze o entrambe.
Differenziare il testing dal debugging.	Cerca le differenze tra i concetti.
Distinguere tra rischi di progetto e rischi di prodotto.	Consente di classificare separatamente due (o più) concetti.
Spiegare l'impatto del contesto sul processo di test.	
Fornire esempi del perché il testing è necessario.	
Inferire la root cause dei difetti a partire da un dato profilo di failure.	
Riassumere le attività del processo di review dei prodotti di lavoro.	

Livello 3: Applicare (K3)

Il candidato è in grado di eseguire una procedura quando si trova di fronte a un compito che gli è familiare, oppure di selezionare la procedura corretta e applicarla a un determinato contesto.

Verbi di azione: applicare, implementare, preparare, utilizzare

Esempi	Note
Applicare l'analisi dei valori limite per derivare i test case da dati requisiti.	Dovrebbe riferirsi a una procedura / tecnica / processo ecc.
Implementare metodi di raccolta delle metriche a supporto dei requisiti tecnici e gestionali.	
Preparare i test di installabilità per le app mobile.	
Utilizzare la tracciabilità per monitorare l'avanzamento del test quanto a completezza e consistenza rispetto agli obiettivi del test, alla strategia di test e al test plan.	Può essere utilizzato in un obiettivo di apprendimento che richiede al candidato di essere in grado di utilizzare una tecnica o una procedura. Simile a "applicare".

Riferimento

(Per i livelli cognitivi degli obiettivi di apprendimento)

Anderson, L. W. and Krathwohl, D. R. (eds) (2001) A Taxonomy for Learning, Teaching and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Allyn and Bacon

10 Appendice B – Matrice di Tracciabilità dei Business Outcome rispetto agli Obiettivi di Apprendimento

Questa sezione elenca la tracciabilità tra i Business Outcome e gli Obiettivi di Apprendimento del Certified Tester - Finance Testing.

Business Outcome: Certified Tester - Finance Testing			BO1	BO2	BO3	BO4	BO5	BO6
BO1	comprendere la struttura del settore finanziario, i suoi istituti, sistemi e processi e spiegare le sfide specifiche del testing all'interno di questo dominio.		4					
BO2	applicare pratiche di test che supportano la conformità alle normative e agli standard finanziari, verificando che siano soddisfatti i requisiti di auditability, tracciabilità e documentazione.			7				
BO3	applicare il testing basato sul rischio ai sistemi finanziari, prioritizzando le attività di test in base ai rischi di business, tecnici e normativi.				3			
BO4	comprendere le pratiche di test che verificano l'accuratezza, la consistenza e la protezione dei dati nei sistemi finanziari, incluso l'uso di tecniche di masking e di anonimizzazione.					4		
BO5	applicare le tecniche di test funzionali e non-funzionali tipicamente utilizzate nel dominio finanziario, con particolare attenzione agli aspetti non-funzionali quali prestazioni, affidabilità e sicurezza.						5	
BO6	comprendere il ruolo della test automation negli ambienti finanziari e applicare efficacemente le strategie di test automation sia nei sistemi legacy sia in quelli moderni, tenendo conto dei vincoli normativi.							4

LO univoco	Obiettivo di Apprendimento	Livello K						
1	Introduzione al Settore dei Servizi Finanziari							
1.1	Fondamenti del Testing del Software nel Finance Testing							
FT-1.1.1	Richiamare gli obiettivi primari del finance testing	K1	X					
FT-1.1.2	Riassumere le caratteristiche peculiari e i requisiti tecnici dei vari ambienti di test finanziari	K2	X					
FT-1.1.3	Identificare i principali sistemi finanziari e i workflow testabili tipicamente associati a essi	K2	X					
1.2	Sfide e Ruolo della Conoscenza del Dominio nel Finance Testing							
FT-1.2.1	Spiegare come la conoscenza del dominio viene applicata per mitigare le sfide comuni del testing nel settore finanziario	K2	X					
2	Testing di Conformità							
2.1	Obiettivi e Approcci del Testing di Conformità							
FT-2.1.1	Riassumere gli obiettivi del testing di conformità e la relazione tra i suoi principali approcci del test	K2		X				
2.2	Le Normative Finanziarie e il Loro Impatto sul Testing							
FT-2.2.1	Spiegare la rilevanza per il testing delle principali normative e standard finanziari	K2		X				
FT-2.2.2	Richiamare le conseguenze della non-conformità alle normative finanziarie	K1		X				
2.3	Caratteristiche Distintive del Finance Testing Regolamentato							
FT-2.3.1	Riassumere le caratteristiche peculiari del finance testing	K2		X				
2.4	Auditability e Validazione Continua Automatizzata della Conformità							
FT-2.4.1	Comprendere i principi fondamentali dell'auditability nel testing di conformità	K2		X				

FT-2.4.2	Comprendere i principi e i meccanismi di implementazione della Validazione Continua Automatizzata della Conformità (CACV) all'interno del ciclo di vita di consegna del software.	K2		X				
3	Testing Basato sul Rischio							
3.1	Categorie di Rischio nei Sistemi Finanziari							
FT-3.1.1	Spiegare le principali categorie di rischio nei sistemi finanziari	K2			X			
3.2	Principi del Testing Basato sul Rischio in Ambito Finanziario							
FT-3.2.1	Spiegare i principi del testing basato sul rischio in ambito finanziario	K2			X			
3.3	Attività Basate sul Rischio							
FT-3.3.1	Spiegare come la prioritizzazione basata sul rischio influisce sulle attività di test nelle applicazioni finanziarie	K2			X			
4	Testing dei Dati e Gestione dei Dati							
4.1	Accuratezza e Consistenza dei Dati							
FT-4.1.1	Spiegare l'importanza dell'accuratezza e della consistenza dei dati nei sistemi finanziari	K2				X		
4.2	Riconciliazione dei Dati tra Sistemi Finanziari							
FT-4.2.1	Applicare le tecniche di riconciliazione dei dati ai processi finanziari multi-sistema	K3				X		
4.3	Data Privacy e Protezione dei Dati nel Finance Testing							
FT-4.3.1	Spiegare l'importanza della data privacy e della protezione dei dati nel finance testing	K2				X		
5	Testing Funzionale e Non-Funzionale							
5.1	Testing Funzionale dei Sistemi Finanziari							
FT-5.1.1	Applicare il testing funzionale per validare i sistemi finanziari	K3					X	
5.2	Rischi di Prestazione in Ambito Finanziario							

FT-5.2.1	Spiegare i rischi di prestazione nei sistemi finanziari durante i periodi di picco	K2					X	
5.3	Performance Testing in Contesti Finanziari							
FT-5.3.1	Applicare il load testing e lo stress testing in contesti specifici del settore finanziario	K3					X	
5.4	Testing di Sicurezza e Testing di Disponibilità							
FT-5.4.1	Spiegare le esigenze di testing di sicurezza e testing di disponibilità nei sistemi finanziari	K2					X	
5.5	GenAI nel Testing del Software Finanziario							
FT-5.5.1	Spiegare come la GenAI può supportare e migliorare il finance testing	K2					X	
6	Test Automation							
6.1	Ruolo della Test Automation nel Finance Testing							
FT-6.1.1	Spiegare come la test automation supporta l'efficienza dei test in ambito finanziario	K2						X
6.2	Strategie di Test Automation							
FT-6.2.1	Applicare le strategie di test automation in panorami IT finanziari legacy e moderni	K3						X
6.3	Sfide della Test Automation in Ambienti Regolamentati							
FT-6.3.1	Spiegare le sfide della test automation in ambienti regolamentati	K2		X				X
6.4	Sfide nei Diversi Tipi di Test Automation							
FT-6.4.1	Spiegare le sfide della test automation su componenti mobile, frontend e backend	K2						X

11 Appendice C – Note di Rilascio

Il Syllabus ISTQB® Certified Tester – Finance Testing (CT-FT) v1.0 è il primo rilascio di questo syllabus Specialist. Introduce un approccio strutturato al testing nel dominio finanziario, affrontando le sfide peculiari dei sistemi, dei processi e dei requisiti normativi finanziari.

La realizzazione di questo syllabus nasce dalla crescente dipendenza del settore finanziario da panorami IT complessi, dalla crescente importanza della conformità normativa e dalla domanda di approcci del test basati sul rischio e centrati sui dati.

Questo rilascio si propone di fornire a organizzazioni finanziarie, tester e professionisti della qualità una conoscenza pratica e specifica del dominio, che completa il portafoglio ISTQB® esistente.

Scopo e benefici

Il syllabus CT-FT rafforza il portafoglio ISTQB® affrontando uno dei settori più regolamentati e critici al mondo. Consente ai tester di acquisire una preziosa competenza di dominio, supporta le organizzazioni nel soddisfare i requisiti di conformità e di qualità e contribuisce al riconoscimento professionale del finance testing in tutto il mondo.

Trattandosi di un primo rilascio, CT-FT stabilisce la base di riferimento per gli aggiornamenti futuri. Le evoluzioni seguiranno le tendenze del settore, gli sviluppi normativi e le tecnologie emergenti, per contribuire a mantenere il syllabus rilevante sia per i professionisti sia per le organizzazioni.

12 Appendice D – Indice Analitico

accettazione del rischio; 29
accuratezza dei dati; 31
accuratezza funzionale; 14
ambiente; 32; 50
analisi dei requisiti; 21
analisi dei valori limite; 37
Anti-Money Laundering; 16
auditability; 22
Basel III/IV; 20
campionamento dei record; 32
compliance as code; 23
condizione di test; 17; 28
conformità normativa; 14
confronto di aggregati; 32
consistenza dei dati; 31
continuous control monitoring; 23
copertura; 28
core banking system; 15
criteri di accettazione; 17
dati di test; 17
Digital Operational Resilience Act; 20
Direttiva antiriciclaggio; 20
evitamento del rischio; 28
fiducia del cliente; 14
General Data Protection Regulation; 20
Generative AI; 50
gestione dei dati di test; 22
impatto del rischio; 27
instabilità; 50
integrità dei dati; 14
integrità delle evidenze; 23
ISO 20022; 15
ISO 31000; 29
ISO/IEC 25010; 26
ISO/IEC 25019; 26
livello di rischio; 27
Markets in Crypto-Assets Regulation; 20
migrazione dei dati; 32
mitigazione del rischio; 28
normative finanziarie; 20
oracolo del test; 16
partizionamento di equivalenza; 37
Payment Services Directive 2; 20
penetration testing; 42
pipeline di CI/CD; 23
piramide di test; 50
privacy; 23
probabilità del rischio; 27
protocollo FIX; 15
regression testing automatizzato; 48
riconciliazione dei dati; 32
rilevamento dei difetti; 28
riproducibilità; 23
rischio; 21
rischio di prodotto; 26
rischio di progetto; 26
Sarbanes-Oxley Act; 20
scanning delle vulnerabilità; 42
shift-left; 47
sicurezza; 14
spike testing; 41
stress testing; 41
strumenti; 49
test case; 17

testing back-to-back; 38
testing basato sul rischio; 17
testing dei calcoli; 38
testing della tabella delle decisioni; 37
testing delle transizioni di stato; 37
testing di conformità normativa; 21
testing di controllo; 19
testing di disponibilità; 42
testing di scalabilità; 41
testing di sicurezza automatizzato; 50

testing esplorativo; 38
testing guidato dalle evidenze; 22
testing negativo; 22
testing non-funzionale; 22
testing sostanziale; 19
tracciabilità; 22
trasferimento del rischio; 29
validazione continua automatizzata della
conformità; 23
verifica dei checksum; 32