Automated Testing of Controls

www.hexaware.com

Financial and Operational Internal Controls – A background

What are internal controls?

Financial and operational Internal Controls form the backbone of all businesses. They ensure that daily operational procedures are followed exactly as intended to achieve required internal and regulatory compliance. A control in any process has two aspects:

- The right outcome it intends to achieve
- The wrong outcome it intends to prevent

An example of an operational control can be - authentication to access software systems running business processes, where authorized users are allowed access, while unauthorized users are denied access. Similarly, financial controls can relate to the capture, classification and presentation of financial accounting transactions, requiring appropriate authorization, and oversight from top management.

Internal Controls can be preventative (don't allow errors to occur), detective (spot errors that have occurred), and/or corrective (fix errors) – depending on the purpose they serve.

Process Digitization and Automation of Controls

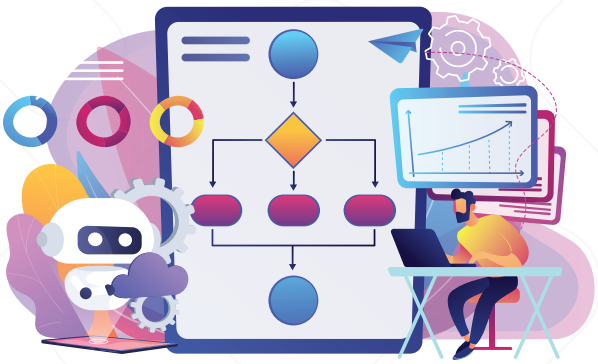
Manual controls create more operational risk as they can be executed by unauthorized personnel or, in some cases, authorized personnel in erroneous or fraudulent ways. With most businesses digitizing their processes, a significant proportion of controls are embedded in software, and their execution is automated with an audit trail generated. At the step where this process has a hand-off to/from a manual process, consequently increasing risks can be mitigated with appropriate checks and balances, such as by reconciling manual pieces of the process with the digitized process in cases where automation of a manual process or controls therein is not feasible.

Testing of Controls and the case for automation

Testing of Controls is a critical activity undertaken at regular intervals or when there are significant changes to business procedures. It is a time-consuming activity and a tremendous drain on the resources of an organization. Outdated documentation of internal controls creates risks to business itself, and compliance audits may be impeded – resulting in internal or regulatory non-compliance risks.

Therefore, a strategic approach to automated controls testing can go a long way in reducing risk.

Business operations form the First Line of Defence for any organization. The Second Line of Defence or Internal Compliance function validates and maintains the rigour around all internal controls for business processes. The Third Line of Defence or the Internal Audit function has the responsibility to periodically verify that business procedures were adhered to (in the audit period under scrutiny). Together, these functions roll up to the Head of Risk in an organization. Hence, an overarching strategy that involves stakeholders within all lines of defence is likely to be more effective than one driven by the Compliance function alone.



The Three Lines of Defense in Enterprise Risk

CFO **CEO** **Board**

Risk Appetite Framework (RAF) based comprehensive & dynamic oversight

Chief Risk Officer (CRO)

Executive level sponsorship for risk

First Line of Defense (Business Units)

Conduct day-to-day business with agreed risk rigour & a conducive control environment

- Risk ownership and complying to
  - Procedural steps
  - Approval levels
  - Key risk indicators (KRIs), inc. limits & thresholds
- Strategy guidance for internal controls formulation
- Own & drive RCSA (business self-assessment)

Second Line of Defense (Internal Compliance)

Independently assess and challenge risk contribution by Business and escalate to Board level

- Institute risk management practices with operational standards, taxonomy, risk frameworks, methodologies & models
- New risk identification for business environment & regulation changes
- Risk monitoring, aggregation & reporting (internal/regulatory)
- Advising and training Business

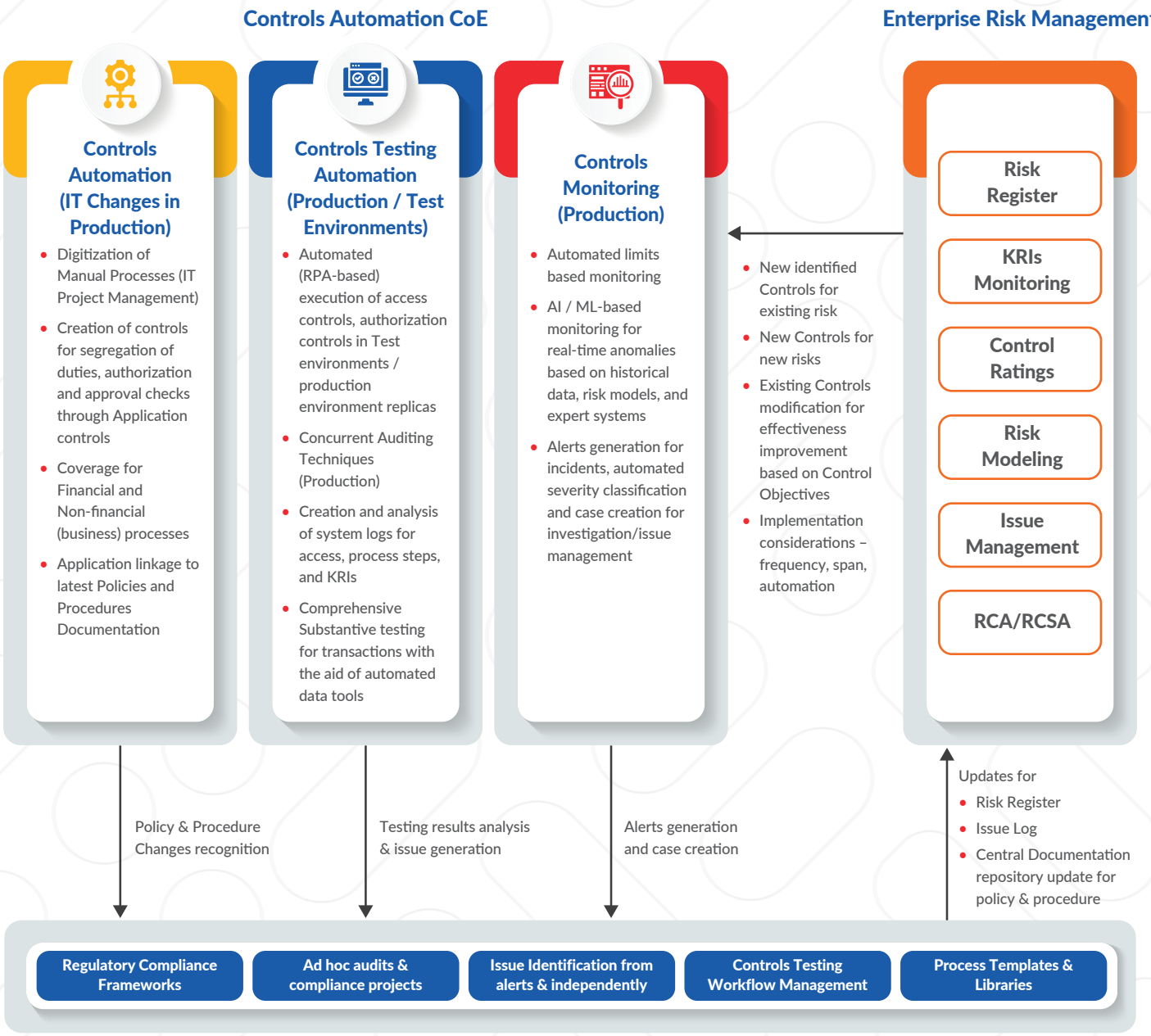
Third Line of Defense (Internal Audit & Assurance)

Independently review and challenge levels of efficacy & adherence of processes & controls

- Periodic verification & validation of control objectives, controls & execution
- Objective guidance for first two lines to rationalize and optimize controls
- Independent reporting to board to support internal control framework
- Key risk detection through audit activities & enhancing enterprise efficiency

Hexaware's PoV – Testing of Controls Automation

A CoE-driven approach specifically targeted at testing of controls can improve risk management and achieve reduced TCO over the long term by developing a platform that integrates seamlessly with business and risk functions.



Once uniquely identified, all risks and corresponding compliance requirements can be mapped to individual controls – in a clear and unambiguous one-to-many mapping format (where the same control meets different compliance requirements, at times).

Specific and up-to-date documentation mapped to risk identifiers (and controls) helps ensure accurate measurement of the efficacy of controls – this, in turn helps manage and keep pace with ever-changing, ever-evolving business, operational and regulatory changes.

Through a centralized platform and with a three-pronged approach – Controls Automation, Controls Testing Automation, and Controls Monitoring – organizations can negotiate emerging risks by managing all compliance requirements, controls, documentation, and issues detected.

Automation of controls can be achieved through three broad mechanisms (or a mix thereof, depending on specific compliance requirements)

- The 'Continuous Audit' approach where transactions in business applications are examined in real-time to check for fraud or operational errors. This would be particularly useful for large value transactions that must be prevented if executed against the intent of the procedure. This can also include dummy transactions to check the entire lifecycle of the transaction but without financial impact.
- Post-facto testing, where transactions are checked after execution or completion.
- Testing controls in production environment replicas, with exact images of production environment (application code and data), such that there is no risk to production environments, but the test results would be equally effective in identifying issues.

An integrated approach such as this, will ensure plenty of benefits:

A Single view of all organizational internal controls, with mechanisms to ensure that procedures followed are current, and risk is quantified at appropriate levels before being accepted at the designated risk appetite.

Highest levels of transparency – internally and for external stakeholders (customers, investors, and regulators).

Up-to-date risk register as well as effective RCAs (Risk & Control Assessments) and RCSAs (Risk & Control Self-Assessments).

Reduced internal and external audit completion time.

Repeatable results in case of framework-based compliance exercises such as SOX, PCI-DSS, and the like.

Conclusion

Testing of control automation can transform risk and compliance functions to improve cost efficiencies, resilience, and performance. It is the need of the hour, taking into consideration evolving business models and the advent of new technologies and the need to reduce risks and optimize cost. With Hexaware's deep-rooted automation-first approach hinged on our Automate Everything™ strategy, banking and financial services companies can leverage our integrated, end-to-end testing of controls solutions to disrupt risk and compliance management, and gain business advantage.

For more insights, do get in touch with our automation experts to reimagine risk and compliance management. Email: marketing@hexaware.com

References

Accounting Tools (2019). Test of Controls. Retrieved from
https://www.accountingtools.com/articles/what-are-tests-of-controls.html

Deloitte. Digital testing and controls automation. Retrieved from
https://www2.deloitte.com/us/en/pages/advisory/articles/digital-testing-approach.html

Cyber Experts. IT Auditing – Planning the IT Audit. Retrieved from
https://cyberexperts.com/it-audit/

Accounting Financial & Tax. Techniques and Technology Used In Auditing. Retrieved from.
http://accounting-financial-tax.com/2009/11/techniques-and-technology-used-in-auditing/

Deloitte (2018). The Future of IT Internal Controls – Automation: A Game Changer. Retrieved from
https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-future-of-it-internal-controls-noexp.pdf

Audit Board (2020). Audit Management Playbook. Retrieved from
https://www.auditboard.com/blog/audit-management-playbook/

https://promontory.com/our-expertise/article/5fd77d8d50a91c0a9283d3d4

Authors

- Alok Mishra, Principal Consultant, Hi-Tech & Professional Services, Hexaware Technologies
- Arun Narayanan, AVP & Practice Head, Hi-Tech & Professional Services, Hexaware Technologies

About Hexaware

Hexaware is the fastest growing next-generation provider of IT, BPO and Consulting services. Our focus lies on taking a leadership position in helping our clients attain customer intimacy as their competitive advantage. Our digital offerings have helped our clients achieve operational excellence and customer delight. We are now on a journey of metamorphosing the experiences of our customer's customers by leveraging our industry-leading delivery and execution model, built around the strategy— AUTOMATE EVERYTHING®, CLOUDIFY EVERYTHING®, TRANSFORM CUSTOMER EXPERIENCES®. Hexaware services customers in over two dozen languages, from every major time zone and every major regulatory zone. Our goal is to be the first IT services company in the world to have a 50% digital workforce.
Learn more about Hexaware at http://www.hexaware.com

NA Headquarters
Metro 101, Suite 600,101
Wood Avenue South, Iselin,
New Jersey - 08830
Tel: +001-609-409-6950
Fax: +001-609-409-6910

India Headquarters
152, Sector – 3
Millennium Business Park
'A' Block, TTC Industrial Area
Mahape, Navi Mumbai – 400 710
Tel : +91-22-67919595
Fax : +91-22-67919500

EU Headquarters
Level 19, 40 Bank Street,
Canary Wharf,
London - E14 5NR
Tel: +44-020-77154100
Fax: +44-020-77154101

APAC Headquarters
Asia Pacific Pte Ltd,
#09-01, 1 Finlayson Green
Singapore-049246
Tel : +65-63253020
Fax : +65-6222728

Australia Headquarters
Level 3, 80 Mount
North Sydney
NSW 2060, Australia
Tel : +61 2 9089 8959
Fax : +61 2 9089 8989

Safe Harbor Statement
Certain statements in this press release concerning our future growth prospects are forward-looking statements, which involve a number of risks, and uncertainties that could cause actual results to differ materially from those in such forward-looking statements. The risks and uncertainties relating to these statements include, but are not limited to, risks and uncertainties regarding fluctuations in earnings, our ability to manage growth, intense competition in IT services including those factors which may affect our cost advantage, wage increases in India, our ability to attract and retain highly skilled professionals, time and cost overruns on fixed-price, fixed-time frame contracts, client concentration, restrictions on immigration, our ability to manage our international operations, reduced demand for technology in our key focus areas, disruptions in telecommunication networks, our ability to successfully complete and integrate potential acquisitions, liability for damages on our service contracts, the success of the companies in which Hexaware has made strategic investments, withdrawal of governmental fiscal incentives, political instability, legal restrictions on raising capital or acquiring companies outside India, and unauthorized use of our intellectual property and general economic conditions affecting our industry.

© 2020 Hexaware Technologies limited. All rights reserved.