Deloitte.

Findings Lifecycle Management
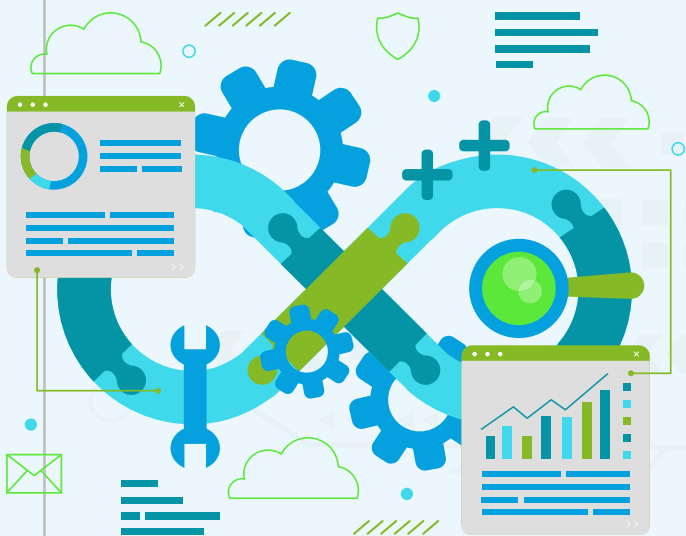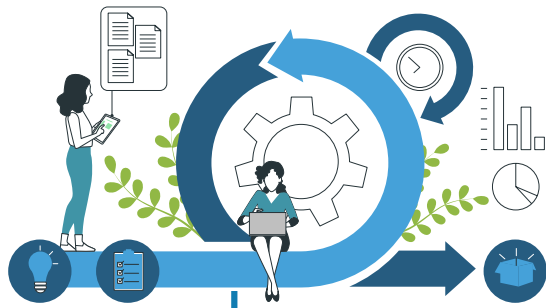
Mitigating risks. Building resilience.

Organisations are constantly looking to expand their footprint, widen their customer base and garner more revenue. The ever-changing legal and regulatory obligations require organisations to constantly be on their toes with respect to compliance. They need to keep updating their security practices, to mitigate the risks presented by advanced threat vectors.

Absence of robust cybersecurity frameworks, ineffective communication, and a lack of awareness towards cyber leads to a multitude of risks that need to be mitigated. Failure to mitigate these issues/findings leads to accumulation, which will have a substantial impact on the organisation's security health, operations, legal and reputation, and compliance.

These accumulated and untreated issues/findings can lead to unknown risk exposure to the firm. These untreated findings may lead to a cyber incident or a breach which has the potential to directly deplete an organisation's resources, cause a decline in the organisation's credit rating, adversely impact the organisation's ability to secure financial backing from stakeholders and shareholders, leading to increased expenses.

These findings can be categorised into multiple domains, such as:

Findings

- Cybersecurity
- Data Privacy
- Data Protection
- Vendor and Supply risk
- Cloud Security
- Regulatory and Legal
- Enterprise Resilience
- Application Security

There are multiple factors that contribute significantly to the ineffective management of findings within an organisation. These include and are not limited to:

- Poor findings governance
- Ineffective findings monitoring due to unknown number and type of findings (no repository)
- Not utilising tools and technology (GRC)
- Weak policies
- Unclear accountability
- Ineffective communication
- Insufficient resource/budget allocation issues
- Changing regulatory/compliance requirements
- Lack of training and awareness

Findings Lifecycle Management (FLM)
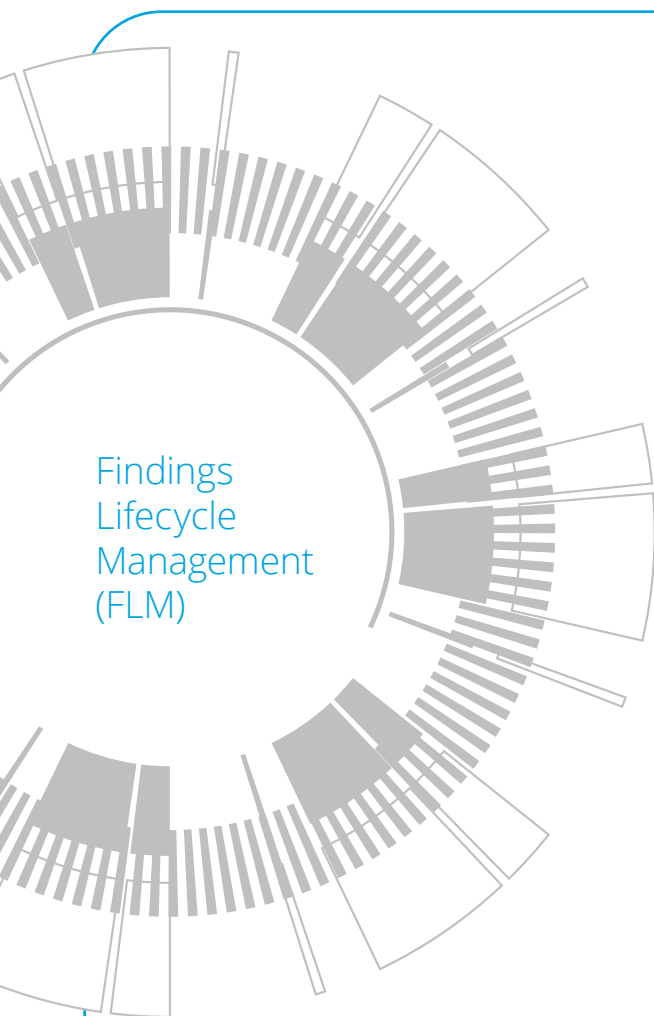
Finding Lifecycle Management focuses on improving the overall governance of security findings and exceptions (if any) by providing direction, recommendations, and coordination with the finding owners (FO) through crisp and precise communication to mitigate or remediate open findings. Effective findings management is an indispensable element of a holistic cybersecurity strategy of the organisation. It not only ensures the immediate mitigation of risks but also bolsters the organisation's long-term resilience by:

Findings Lifecycle Management

Increasing stakeholders' trust

Reducing Security Risks

Better Accountability

Effective Decision Making

Enhance Resilience

Improved Compliance

Findings Lifecycle Management will support the organisations in:

Developing strategies to mitigate identified risks, reducing the likelihood of disruptions, financial losses, and reputational damage. It is more economical to prevent security incidents rather than deal with the consequences of a breach, which may entail expenses related to legal matters, regulatory penalties, and impact the organisation's reputation. Financial penalties can go up to **10 - 20 million Euros,** or **2 percent** of the annual revenue in case of GDPR, or up to **250 Cr INR** (approx. USD $30 million) for non-compliance to India's DPDP Act.

Safeguarding sensitive and confidential information, by adequately addressing security concerns to prevent any potential data exposure or compromise. This will protect an organisation's valuable assets and ensure the trust of both customers and stakeholders.

Creating an actionable remediation or mitigation plan which can support findings owners by providing better service to end users. A well- structured findings process guarantees a quicker and more efficient response to minimise consequences and time required for recovery during the incidents.

Contributing to effective communication flows within the organisation, which translates to more accurate information and responses to the finding owners.

Ensuring continuity of services throughout the year and minimising disruptions that could negatively impact end users. It is essential to address security vulnerabilities and risks to prevent any potential disruptions to business operations and reduce the impact of potential incidents.

Enabling effective governance by reducing open risks, enhancing customer satisfaction, and achieving sustainable success.

Effectively prioritising and managing findings, which ensures that issues are tackled promptly, optimising time and cost.

Proper identification and effective management of findings within an organisation is of utmost importance to uphold a robust security stance and tackle any vulnerabilities and risks that may arise.

The Deloitte difference:

- Experienced in building and running Findings Lifecyle Management programmes.
- Cyber analytics capabilities for continuous monitoring and predictive analysis, to effectively manage the problem at a governance layer.
- Security automation for automated response to certain type of findings to expedite the mitigation process.
- Behavioral analysis for early detection of potential security findings.
- Cyber analytics qualified and certified professionals with relevant experience in cyber and stakeholder management.
- Tool agnostic approach, proficient at multiple GRC and finding management tools.
- Quick ramp-up/down of the team based on the demand.
- Focused point of contacts for across business areas/verticals, ensuring better governance of findings.
- A dedicated Center of excellence (COE) for technical remediation consultation.
- SLA-driven approach for closure of findings and proven improved efficiencies through regular governance and close monitoring.
- Effective reporting and dashboarding, including persona-based reporting.
- Creation/updation of relevant documents, and process flows, related to finding management.
- Continuous improvements and efficiency-driven processes.

Conclusion
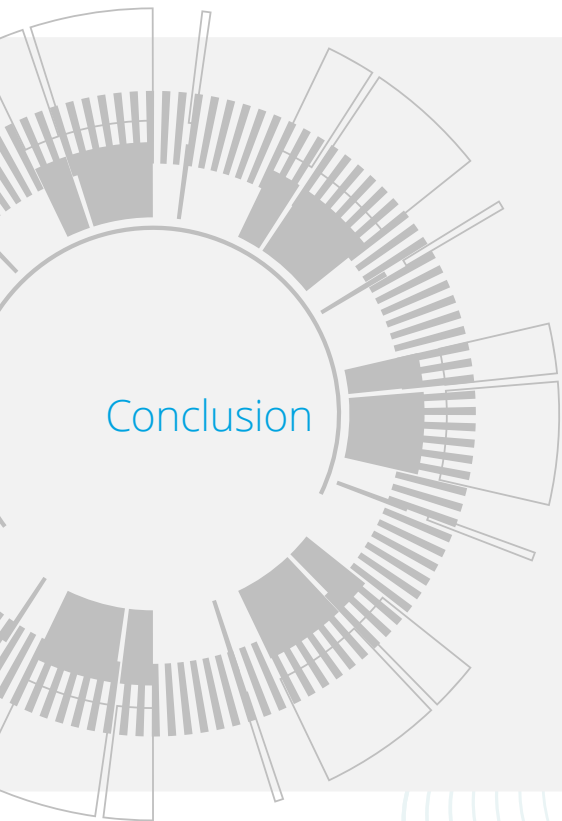
An efficient management of findings serves as the cornerstone of a robust and protected organisational structure. By giving priority to identifying and promptly addressing vulnerabilities and risks, not only can cybersecurity threats be mitigated, but sensitive data can also be safeguarded, regulatory compliance can be ensured, and the organisation's reputation can be preserved.

Through promoting uninterrupted operations, reducing expenses, and improving incident response capabilities, organisations can inspire confidence among stakeholders and gain a competitive advantage. Ultimately, taking a proactive approach to findings management is in line with strategic decision-making, empowers employees, and positions the organisation to adapt to the ever-changing landscape of cybersecurity threats.

Connect with us:

Sathish Gopalaiah
Partner, Deloitte India
sathishtg@deloitte.com

Deepa Seshadri
Partner, Deloitte India
deseshadri@deloitte.com

Gaurav Shukla
Partner, Deloitte India
shuklagaurav@deloitte.com

Munjal Kamdar
Partner, Deloitte India
mkamdar@deloitte.com

Sowmya Vedarth
Partner, Deloitte India
sovedarth@deloitte.com

Key contributor: Aditya Saxena

Deloitte.