Reporting With Impact: IT

Visibility into IT risk, compliance, and performance shouldn't rely on guesswork. This guide outlines what leadership and Boards should be seeing in regular IT reports to support informed, confident decisions.

Leadership (Operational & Tactical)	Board (Strategic & Risk Governance)

Cybersecurity Posture

Leadership (Operational & Tactical)

- Key cybersecurity incidents, responses, and lessons learned
- Key cyber controls updates
- Insider and external threat intelligence

Board (Strategic & Risk Governance)

- High-level cyber risk assessment
- Framework compliance (e.g., NIST, ISO 27001, SOC 2)
- Cyber resilience strategy

Regulatory Compliance & Legal Risks

Leadership (Operational & Tactical)

- IT compliance effort updates (e.g., SOX 404, PIPEDA, CSA246.1)
- Internal control assessments and remediation progress

Board (Strategic & Risk Governance)

- Summary of regulatory risks and compliance status
- Major IT-related legal or compliance risks

IT / OT Risk Management

Leadership (Operational & Tactical)

- Active and emerging IT risks (cloud, supply chain)
- Incident and outage trends with root cause analyses
- Risk register & mitigation updates

Board (Strategic & Risk Governance)

- Strategic IT risk outlook
- Business continuity & disaster recovery status
- Third-party/vendor risk management

IT / OT & Cybersecurity Metrics (KPIs/KRIs)

Leadership (Operational & Tactical)

- Patch management compliance %
- Mean time to detect/respond (MTTD/MTTR)
- Pen test results & remediation progress
- System uptime/performance

Board (Strategic & Risk Governance)

- Industry benchmarking (e.g. against peers, or cybersecurity frameworks)
- Cyber insurance coverage and risk exposure assessment

Reporting With Impact: IT

Leadership (Operational & Tactical)	Board (Strategic & Risk Governance)

IT Budget & Investments

- IT and security spend vs. budget
- ROI on major IT initiatives
- Cost-benefit analysis of new technology investments

- Alignment of IT spend with business strategy
- Cybersecurity investment strategy and risk-based prioritization

Major IT Projects & Digital Transformation

- Progress updates on key IT projects
- Project risks, delays, or budget overruns
- User adoption and change management status

- Strategic IT initiatives aligned with business growth
- Risks/opportunities from digital transformation efforts
- Technology trends impacting the company's competitive position

Incident Response & Crisis Preparedness

- Recent security incidents and mitigation steps
- Status of disaster recovery and business continuity testing
- Readiness drills and response capabilities

- Cyber incident reporting protocol for
- material breaches
- Crisis management preparedness and
- Board-level engagement plan

Emerging Technologies & Threat Landscape

- AI, IoT, OT and blockchain risks and opportunities
- Threat intelligence reports from security partners
- IT department skill gaps and training updates

- Board education on key IT and cybersecurity trends
- Strategic discussions on emerging risks (e.g., AI-powered cyber threats)