Science & Technology · GS - III

Legacy information technology systems continue to pose operational and cybersecurity challenges for governments and critical infrastructure. Examine the risks associated with their modernisation and suggest measures to ensure a secure and resilient digital transition.

EXAM YEAR	PAPER	SUBJECT
DAILY PRACTICE 23/11/2026	GS - III	Science & Technology

MARKS	WORD LIMIT
15	~250 words

Answer Hint

Legacy infrastructure, interoperability, cybersecurity vulnerabilities, service continuity, cloud migration, disaster recovery, digital resilience

Model Answer

Introduction

Legacy information technology systems are older hardware and software platforms that continue to support essential services. Their modernisation is necessary for efficiency and security, but poorly managed transitions can cause service outages, data loss and operational vulnerabilities.

Major Challenges of Modernisation

1. **System incompatibility:** Older platforms may not integrate easily with modern applications, databases and cloud-based infrastructure.

2. **Cybersecurity vulnerabilities:** Unsupported software, outdated encryption and unpatched systems can expose sensitive information to cyberattacks.

3. **Service disruption:** Migration errors, software incompatibility and inadequate testing can interrupt essential public and private services.

4. **Skill and cost constraints:** Modernisation requires substantial investment, specialised personnel and long-term maintenance capabilities.

5. **Vendor dependence:** Reliance on proprietary technologies may create vendor lock-in and reduce flexibility in future upgrades.

Measures for Secure Digital Transition

1. **Phased migration:** Governments should adopt pilot projects, parallel operations and gradual replacement rather than abrupt system-wide transitions.

2. **Cybersecurity by design:** Encryption, multi-factor authentication, regular vulnerability assessments and access controls should be incorporated from the beginning.

3. **Business continuity planning:** Backup infrastructure, disaster recovery sites and tested restoration procedures should protect essential services.

4. **Interoperability standards:** Open standards and secure application programming interfaces can facilitate integration between legacy and modern platforms.

5. **Skilled workforce:** Continuous training and specialised technical teams are essential for managing complex digital transitions.

6. **Accountability and audits:** Independent security assessments, incident reporting and clear responsibility frameworks can strengthen institutional preparedness.

Conclusion

Modernisation is not merely a technological upgrade but a process of strengthening institutional resilience. A phased, secure and well-audited transition can minimise disruptions while improving the reliability of critical digital infrastructure.