A) Exam Snapshot

- Exam: CompTIA Tech+ (FC0-U71) — version V6 | Issuer: CompTIA
- Questions: maximum of 70 | Question types: multiple-choice
- Time limit: 60 minutes | Scoring: scaled 100–900
- Passing score: 650 | Recommended experience: none required

B) Domain Weights

Domain	Weight
Tech concepts and terminology	13%
Infrastructure	24%
Applications and software	18%
Software development concepts	13%
Data and database fundamentals	13%
Security	19%

C) Core Workflow (how the exam thinks)

- Clarify the need: user goal, constraints, and success criteria.
- Map the environment: device, OS, network type, and where data lives.
- Select the right component: hardware, interface, or connection for the requirement.
- Apply safe basics: updates, least privilege, and secure defaults.
- Validate results: connectivity, function, and expected output with quick checks.
- Document and report: what changed, what was tested, and what it means.

D) High-Yield Concepts

- CPU vs RAM vs storage; volatile vs non-volatile.
- Binary and hexadecimal; units of measure (bit/byte; bps/Mbps/Gbps).
- Router vs switch vs firewall; LAN vs WAN; IP vs MAC address.
- Common interfaces: USB, HDMI, Ethernet, Bluetooth, NFC.
- File systems: NTFS vs FAT32 (features and limits).
- Cloud models: SaaS vs PaaS vs IaaS; shared responsibility basics.
- Virtualization: hypervisor and virtual machines (what runs where).
- Databases: relational vs non-relational; table/row/field; keys.
- Security: CIA; authentication vs authorization; password hygiene.
- Encryption: at rest vs in transit (HTTPS/VPN concepts).

E) Common Traps

- Confusing units: bits vs bytes; Mbps vs MBps; GHz vs GB.
- Treating sync as backup; forgetting restore testing.
- Mixing authentication and authorization; skipping least privilege.
- Assuming private browsing equals anonymity or security.
- Jumping to advanced fixes before basic validation (power, cable, restart, known-good).
- Choosing an answer that changes many things instead of the safest verifiable next step.

F) Cheat Sheet (quick recognition)

- CIA: confidentiality, integrity, availability (what risk is being reduced).
- AuthN vs AuthZ; MFA factors (know, have, are).
- Encryption at rest vs in transit; HTTPS and VPN are transit examples.
- Backup types: full, incremental, differential (time vs restore trade-offs).
- HDD vs SSD/NVMe (spinning vs flash; typical performance differences).
- Wi-Fi: 2.4 GHz range vs 5 GHz speed; interference and channel overlap.
- Database nouns: query returns records; report presents results for humans.
- Troubleshooting loop: identify -> test -> fix -> verify -> document.

G) Exam-Day Tactics

- Answer fast wins first; flag time-sinks; protect your last 10 minutes.
- Read the last sentence first to find the task (best next step, likely cause).
- Eliminate risky options: big changes without validation; “always/never” wording.
- Prefer verifiable actions: check settings, status, and basics before reconfiguring.
- Match constraints: device type, OS, network, and user goal drive the best choice.
- If stuck, pick between the last two by what is safest and testable.
- Review flagged items; change answers only with a clear, concrete reason.

H) 30-Minute Final Review Plan

- 5 min: skim domain weights; prioritize Infrastructure and Security.
- 7 min: walk one scenario end-to-end (device + network + data + security).
- 6 min: drill distinctions (CPU/RAM/storage; IP/MAC; router/switch/firewall; AuthN/AuthZ).
- 6 min: review databases, file systems, cloud models, and virtualization terms.
- 6 min: scan traps list; commit to “verify first, change second.”