SOX is a great differentiator in GRC interviews. Here’s a tight but thorough, interview-oriented guide you can master in a day and speak confidently.

**SOX, End-to-End (Interview Edition)**

**1) What SOX is (and isn’t)**

* **SOX = Sarbanes-Oxley Act (US, 2002)**: law to protect investors by improving **ICFR** (Internal Control over Financial Reporting).
* **Two key sections**:
  + **§302**: CEO/CFO certify disclosure controls each quarter.
  + **§404**: Management assesses, and external auditor opines on, **effectiveness of ICFR** annually.
* **Standards & frameworks around it**:
  + **COSO 2013** = the control framework management uses for ICFR.
  + **PCAOB AS 2201** = auditing standard external auditors follow.
  + **COBIT/ITIL** often used to design IT controls supporting ICFR.

**2) What “ICFR” covers**

* Focus is on **financial statement assertions**: **Completeness, Accuracy, Existence/Occurrence, Rights & Obligations, Valuation, Presentation & Disclosure**.
* **Business processes in scope** (typical cycles):
  + **O2C (Revenue/Receivables), P2P (Payables), H2R/Payroll, R2R/Financial Close, Inventory/Costing, Treasury/Tax**.
* **IT systems** supporting these cycles (ERP, sub-ledgers, data warehouses) + **EUCs** (critical spreadsheets, Access DBs).

**3) Scoping & Planning (how programs really start)**

* **Top-down risk assessment**:
  1. Identify **significant accounts & disclosures** (materiality-driven).
  2. Map **relevant assertions** to each account.
  3. Identify **significant processes** and **in-scope systems**.
  4. Determine **Entity-Level Controls (ELCs)** and **ITGCs** to rely on.
* **Materiality**: quantitative threshold used to decide what matters.
* **Reliance strategy**: leverage **ITGCs** so you can rely on **automated controls & IPE** without re-testing the system every time.

**4) Control Types & Language (must know terms)**

* **Manual vs Automated vs IT-Dependent Manual (ITDM)**
* **Preventive vs Detective**
* **Key vs Non-key** (key = mitigates a material misstatement risk)
* **IPE / PBC**: *Information Produced by the Entity* (needs **Completeness & Accuracy** testing) / *Provided by Client* evidence.
* **Attributes** commonly tested: occurrence, completeness of population, approvals, timeliness, accuracy, segregation of duties, evidence of review.

**5) The Big Four of ITGC (core SOX tech controls)**

1. **Logical Access**
   * Joiner/Mover/Leaver (JML), MFA/password policy, privileged access, periodic **UAR** (User Access Review).
   * **Evidence**: access listings (point-in-time + population), tickets/approvals, SoD matrix, UAR sign-offs, log extracts.
2. **Change Management**
   * SDLC, approvals before prod, testing evidence, **segregation between dev/test/prod**, emergency change override & review.
   * **Evidence**: change tickets, approvals, test results, deployment logs (e.g., SAP transports, Git release logs).
3. **Computer Operations**
   * Batch/job monitoring, **backup & restore tests**, incident/problem mgmt, capacity monitoring.
   * **Evidence**: job run logs, failure tickets, backup schedules, restore test reports.
4. **SDLC / New System Implementation**
   * Formal project approval, requirements/design, security involvement, go-live approvals, data migration validation.

**Why ITGCs matter**: If weak, auditors won’t rely on automated controls or IPE → more testing, possible deficiencies.

**6) Business Process Controls (typical SOX “key controls”)**

* **Revenue**: customer master approvals, pricing/rate tables, 3-way match of order–ship–invoice, cut-off review at period end.
* **P2P**: vendor master approvals, PO required, 3-way match (PO/GRN/Invoice), duplicate payment checks.
* **Payroll**: independent review of payroll register, new-hire & termination controls, exception/variance review.
* **R2R/Close**: **account reconciliations** with reviewer sign-off, journal entry approvals (JE policy, thresholds), consolidation review.
* **Inventory**: cycle counts/physical inventory, standard cost updates, write-down reviews.

**Evidence** typically includes: signed reconciliations, JE listing & sampled JEs with support, rate tables with change logs, exception reports with reviewer sign-offs, shipment logs at cut-off.

**7) The Testing Lifecycle (what you’ll actually do/say)**

1. **Walkthrough** (inquiry + observation + inspection): trace a sample transaction **end-to-end**; confirm points where controls occur.
2. **Test of Design (TOD)**: Is the control designed to prevent/detect a material misstatement? Are **who/what/when/how** defined?
3. **Test of Operating Effectiveness (TOE)**: Did it operate as designed for the **full period** at the **stated frequency**?
4. **Sampling**: define **population**, **sampling method**, and **sample size** (e.g., quarterly control → sample 2–3 per year; daily controls → use representative sampling).
5. **Evaluate Deviations**: defect classification, root cause, **compensating controls**.
6. **Deficiency evaluation**: **Likelihood × Magnitude**, aggregate across controls → classify:
   * **Control Deficiency**, **Significant Deficiency**, **Material Weakness**.
7. **Remediation & Retest**: fix design/operation, run for a period, collect new evidence.

**8) Entity-Level Controls (ELCs) you should name in interviews**

* Control environment (tone at the top), code of conduct, **whistleblower hotline**, board/audit committee oversight, anti-fraud programs, enterprise risk assessment, IT governance, policies & training.
* **Why they matter**: strong ELCs can reduce extent of testing; weak ELCs increase risk.

**9) IPE / C&A (the interview trap—answer it cleanly)**

* For any report or spreadsheet used in a control, validate **Completeness & Accuracy**:
  + **Source** (system of record, query ID), **Parameters** (date range, filters), **Integrity** (no manual edits, or change-control if edited), **Reperformance** or **tie-out** to system totals.
* Keep a **“Report Fact Sheet”** per IPE: report name, owner, system, parameters, how completeness & accuracy were tested, evidence location.

**10) SOC 1 Reports (third-party reliance)**

* For outsourced processes (payroll, hosting, SaaS), obtain **SOC 1 Type 2** report.
* Review **opinion, period, complementary user entity controls (CUECs), exceptions, subservice orgs**.
* Confirm your company performs CUECs—this is a common interview check.

**11) Common Interview Topics & Model Phrases**

**Q: Walk me through your SOX testing approach.**  
A: “I start with **scoping via significant accounts** and **relevant assertions**, perform **walkthroughs** to validate points where controls occur, complete **TOD** focusing on who/what/when/how, define populations and sample sizes, perform **TOE** across the full period, test **IPE C&A** for any reports used, evaluate deviations and **deficiency severity**, and support remediation with **retest** evidence.”

**Q: How do you test User Access Reviews (UAR)?**  
A: “I obtain the **population of active users** from the system of record, validate report **C&A**, reconcile to HR roster, sample users to verify **appropriateness vs role** and **manager review sign-off** within SLA; I also check **privileged access**, SoD conflicts, and timely removal for leavers.”

**Q: Change management—what are your must-see artifacts?**  
A: “Approved **change tickets**, **segregation** of developer vs deployer, **test evidence**, **peer review**, and **prod deployment logs**; for emergency changes, I expect **post-deployment approvals** and monitoring.”

**Q: What is a material weakness example?**  
A: “If **user provisioning lacks approvals** and **admin access isn’t reviewed** for the year, increasing risk of unauthorized JEs impacting revenue—given magnitude and likelihood, that could rise to **material weakness**.”

**Q: How do you handle EUCs/spreadsheets in SOX?**  
A: “Maintain **inventory** of key EUCs, enforce **change/version control**, **access restriction**, **logic review**, and **reperformance** of critical calculations.”

**12) Templates you can reuse (quick RCM examples)**

**a) ITGC – Logical Access (Quarterly UAR)**

* **Risk**: Unauthorized access → inaccurate F/S.
* **Control**: Quarterly UAR by process owner; admins reviewed monthly.
* **Test Steps**: Validate C&A of user listing → sample users → confirm appropriateness & approvals → verify leaver removals within X days → evidence of reviewer sign-off.
* **Evidence**: User listing extract, HR terminations, approval emails/tickets, signed UAR pack.

**b) Business Control – Account Reconciliation (Monthly)**

* **Risk**: Misstatement due to unreconciled balances.
* **Control**: Preparer reconciles GL to subledger; reviewer signs within 15 days.
* **Test Steps**: Sample months → inspect reconciliation, tick-and-tie to GL/subledger, check aging of reconciling items, verify reviewer sign-off & timeliness.
* **Evidence**: Reconciliation workpapers, GL/subledger reports, sign-offs with dates.

**13) Frequent Pitfalls (be ready to call these out)**

* Populations not **complete** (e.g., missing users/changes).
* Reviews without **evidence of precision** (no thresholds, no investigation).
* **Late** reviews vs required frequency.
* IPE not validated; screenshots without parameters.
* **Remediation** implemented but not operated long enough to retest.

**14) How your current work maps to SOX (use in your story)**

* Your “green score” tracking ≈ **control completeness & on-time certifications**—position it as **monitoring control performance** and **driving timely remediation**.
* “Reminding control owners” → say you **managed the SOX calendar**, **followed up on PBC items**, and **ensured evidencing** met audit requirements.

**One-Page SOX Study Checklist (use before interviews)**

* Significant accounts & assertions mapped
* ELCs identified
* ITGCs (Access, Change, Ops, SDLC) designed & tested
* Key process controls per cycle (O2C, P2P, R2R, Payroll, Inventory)
* IPE C&A approach documented
* SOC 1 Type 2 review & CUECs tracked
* Sampling logic + period coverage clear
* Deficiency evaluation (MW vs SD) logic
* Close calendar (JE approvals, recons, disclosures) understood