F-010 Fractional Ownership Activity Worksheet

The Pragmatic GRC Methodology™ for SMBs | Resource Library

You don't need to hire a compliance officer. You need to assign each recurring GRC activity to someone who is already close to that work. This worksheet lists the recurring activities from each of the Four Implementation Guides, shows who typically owns each one in a small or midsized business, and gives you space to write down who owns it in yours. That practice is called Fractional Ownership.

How to Use This Worksheet

1. Read each activity and the Typical Owner. Titles describe functions, not required job titles. If you don't have an Operations Manager, write the name of the person who does that work. In many SMBs, that is the Business Owner.
2. Write the person's name in the Your Owner column, and a name in the Backup column so the activity doesn't stop when someone is out.
3. Leave a box blank if no one owns it today. A blank box is useful: it shows where your exposure is. Assign every blank box before you finish.
4. Count the activities each person owns on the Ownership Load Check at the end. If one person owns most of the list, move some of it.
5. Review this worksheet at your Monthly GRC Heartbeat and again whenever someone joins, leaves, or changes roles.

† Separation of duties. Where an activity is marked †, the person who performs the work should not be the only person who verifies it. The Backup column or the Business Owner can serve as the second set of eyes. When no single person controls a sensitive process from start to finish, one mistake or one bad actor can't go unnoticed.

Frequencies follow the verification rhythms in Chapter 6 where the book specifies them. Others are suggested starting points. Adjust them for your size and risk.

Guide 1: Navigate

Know what you own and what depends on it. Primary Living Document: Master Asset Register.

#	Recurring Activity	How Often	Typical Owner	Your Owner (name)	Backup (name)
N-01	Add every new device, application, cloud service, and vendor to the Master Asset Register	Ongoing; confirm weekly	Operations Manager (IT Manager or MSP supplies the details)		
N-02	Review the Master Asset Register for accuracy and confirm every business-critical asset has a named owner	Monthly	Business Owner		
N-03	Review SaaS subscriptions and cloud applications for unapproved tools (Shadow IT)	Quarterly	IT Manager or MSP, with Finance		
N-04	Classify data (Public, Internal, Confidential) and update classifications when new data types appear	Annually and when data changes	Operations Manager		
N-05	Keep the critical vendor list current and documented	Quarterly	Operations Manager, with Finance		
N-06	Confirm who holds root administrative keys and corporate registrar credentials	Quarterly	Business Owner		
N-07	Update the register after acquiring a business, adding a location, or adopting major new technology	As events occur	Business Owner		
N-08	Prepare asset and vendor documentation for a customer security assessment	As requested	Business Owner, with IT Manager or MSP		

Guide 2: Fortify

Turn security policy into technical safeguards. Primary Living Document: Unified System Security Plan.

#	Recurring Activity	How Often	Typical Owner	Your Owner (name)	Backup (name)
F-01	Verify Multi-Factor Authentication (MFA) and Single Sign-On (SSO) are enforced on all required accounts	Quarterly	IT Manager or MSP †		
F-02	Stage and deploy critical security patches within 14 days	Ongoing; check monthly	IT Manager or MSP		
F-03	Review administrative access and apply least privilege (access only to what each role requires)	Quarterly	IT Manager or MSP †		
F-04	Confirm scheduled backups completed and investigate failures	Weekly	Operations Manager or Office Manager		
F-05	Review vulnerabilities and assign a remediation plan to each critical finding	Monthly	IT Manager or MSP		

#	Recurring Activity	How Often	Typical Owner	Your Owner (name)	Backup (name)
F-06	Review hardening of employee devices, cloud environments, and networks	Quarterly	IT Manager or MSP		
F-07	Independently confirm that your MSP is performing the agreed security work	Quarterly	Business Owner †		
F-08	Review the security practices of key technology vendors	Annually	Operations Manager		
F-09	Update the Unified System Security Plan after significant technology changes	After each change; review monthly	IT Manager or MSP, with Business Owner		

Guide 3: Sustain

Keep the business running when disruption occurs. Primary Living Document: Enterprise Risk Register.

#	Recurring Activity	How Often	Typical Owner	Your Owner (name)	Backup (name)
S-01	Review the highest-priority risks in the Enterprise Risk Register and assign owners and due dates	Monthly	Business Owner		
S-02	Track risk burn-down (the pace at which open risks are being closed)	Monthly	Business Owner		
S-03	Test a backup restoration and record the result	Quarterly	IT Manager or MSP, witnessed by Operations Manager †		
S-04	Review and update the Business Continuity and Disaster Recovery plans	Annually	Business Owner, with Operations Manager		
S-05	Run a business continuity exercise (tabletop)	Annually	Business Owner		
S-06	Review incident response roles, contacts, and procedures	Annually	Operations Manager, with IT Manager or MSP		
S-07	Document manual workarounds for outages of key systems (payments, email, cloud platforms)	Annually	Operations Manager		
S-08	Lead triage and communications when a security incident occurs	As incidents occur	Business Owner, with IT Manager or MSP		

Guide 4: Cultivate

Build governance into everyday work and culture. Primary Living Document: Unified System Security Plan.

#	Recurring Activity	How Often	Typical Owner	Your Owner (name)	Backup (name)
C-01	Complete the offboarding checklist and remove all access within 60 minutes of departure	Each departure	Human Resources, with IT Manager or MSP		

#	Recurring Activity	How Often	Typical Owner	Your Owner (name)	Backup (name)
C-02	Confirm that anyone who left in the past week has been fully deprovisioned	Weekly	Operations Manager or Office Manager		
C-03	Deliver security orientation to each new hire during onboarding	Each new hire	Human Resources		
C-04	Review and adjust access whenever someone changes roles	Each role change	Department Manager, with IT Manager or MSP †		
C-05	Send phishing and social engineering micro-quizzes	Every two weeks	IT Manager or MSP, or Compliance/Security Lead		
C-06	Provide role-based security training	Annually, with reinforcement	Human Resources		
C-07	Review user access across all business applications	Quarterly	Department Managers, with IT Manager or MSP †		
C-08	Reinforce governance responsibilities in team meetings	Monthly	Department Managers		

Cross-Cutting: The Management Rhythm

The routines that keep the Three Living Documents and Four Implementation Guides current.

#	Recurring Activity	How Often	Typical Owner	Your Owner (name)	Backup (name)
M-01	Run the Weekly Verification Rhythm (about 15 minutes)	Weekly	Operations Manager or Office Manager		
M-02	Lead the Monthly GRC Heartbeat and update the Three Living Documents	Monthly	Business Owner		
M-03	Review open action items from the previous Heartbeat and reassign overdue work	Monthly	Business Owner		
M-04	Review the Executive GRC Scorecard and Metrics Dashboard	Monthly	Business Owner		
M-05	Hold the quarterly Living Document review	Quarterly	Business Owner, with Operations Manager		

Ownership Load Check

List each person named above and count the activities they own (Your Owner column) and back up (Backup column). Fractional Ownership works when the load is shared.

Person	Role	Activities Owned	Activities Backed Up	Notes (overloaded? no backup?)

Gaps and Next Steps

☐ Activities with no owner (list the IDs): _____

☐ Activities with no backup (list the IDs): _____

☐ Anyone owning more than they can realistically handle: _____

☐ Activities to hand to your MSP or another vendor (confirm in writing): _____

Reviewed by: _____ Date: _____ Next review (Monthly GRC Heartbeat): _____