Practice Guides:
What the Code Looks Like in Action

Practical examples showing how the Code of Professional Conduct can be applied in daily work across key professional areas.

ISC2™

Practice Guides: What the Code Looks Like in Action

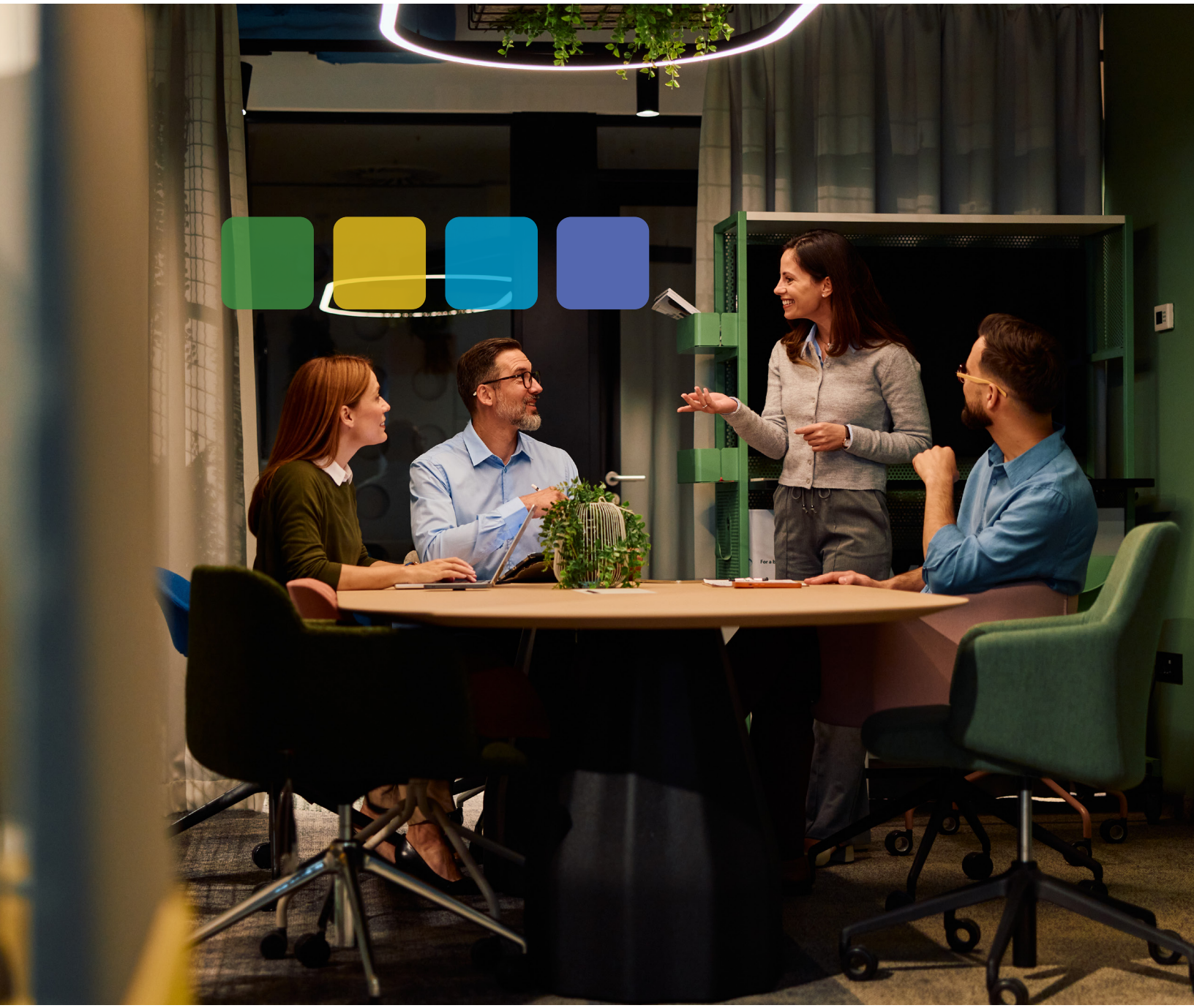
3 **Guide 1:** Commitment to Security and Risk Reduction

4 **Guide 2:** Commitment to Responsibly Securing Emerging Technologies

6 **Guide 3:** Commitment to Balancing Security and Business Objectives

7 **Guide 4:** Commitment to Responsible Use of Privileged Access

Each guide highlights a key area of the Code of Professional Conduct and offers practical examples of behaviors that support ethical, professional practice. Together with the Ethical Decision-Making Guide and a quick self-check, they are designed to support reflection, discussion, and consistent professional practice in real-world situations.



Guide 1: Commitment to Security and Risk Reduction

This guide highlights practices that help cybersecurity professionals reduce risk, strengthen security culture, and communicate clearly in support of the organization's mission.

Effective practices

- Align security with business initiatives and work to reduce risk in support of the organization's mission.
- Encourage all team members to report anything suspicious, regardless of their position in the organization.
- Foster a security-first mindset, emphasizing that security should always be integrated from the start, rather than viewed as an afterthought.
- Provide customized, role-based security awareness training that helps each audience understand and apply secure practices while promoting a culture of security advocacy across the organization.
- Share best practices regularly and, where needed, offer flexible ways to achieve secure outcomes.
- Communicate security risks in business terms that non-technical stakeholders can understand.
- Disclose errors or limitations in findings promptly and transparently.
- Recognize and reward users who have developed or demonstrated good cyber-hygiene practices.

Practices to avoid

- Working in isolation instead of treating security as a shared responsibility.
- Implementing security policies without evaluating their impact on the business.
- Assuming that assigned annual training, completion metrics, or phishing simulation results alone are evidence of effective risk reduction.
- Taking an all-or-nothing approach to risk instead of pursuing secure, practical solutions.
- Departing from best practices without a justified, documented reason.
- Treating security training as a check-the-box exercise rather than an opportunity to build awareness and behavior.
- Focusing only on tools and costs without explaining business impact or risk reduction.

Reflection prompt: What are you already doing well, and based on these examples, what could you start, stop, continue, or change?

Guide 2: Commitment to Responsibly Securing Emerging Technologies

This guide highlights practices that help cybersecurity professionals assess, communicate, and manage the security, privacy, and data risks associated with emerging technologies.

Effective practices

- Develop or support principles-based policies and guidance for the secure use of emerging technologies, with a focus on security, privacy, data protection, acceptable use, risk expectations, and consequences for misuse.
- Ensure that the use of emerging technologies aligns with applicable security, privacy, data protection, regulatory, and standards requirements.
- Help teams understand emerging technologies, the related security, privacy, and data risks, and the safeguards needed to use them responsibly.
- Implement appropriate guardrails to protect sensitive data when adopting emerging technologies.
- Assess and clearly communicate the security, privacy, and data risks of emerging technologies so the business can make informed decisions.
- Maintain visibility into where emerging technologies are being used and regularly review that use to ensure security, privacy, and data risks are monitored, managed, and aligned with current standards, policies, and risk expectations.
- Support governance measures that address the security, privacy, and risk implications of emerging technologies.
- Ensure project teams apply appropriate security, privacy, and data risk considerations when using emerging technologies.
- Validate the security of code, configurations, or outputs produced or influenced by emerging technologies before production use.
- Require appropriate disclosure or labeling of technology-generated content where needed for review, accountability, or risk management.
- Communicate clear expectations for how emerging technologies may be used, including acceptable use, required safeguards, escalation points, and consequences for misuse.
- Incorporate guidance and training on the secure use of emerging technologies into onboarding and ongoing awareness efforts, updating it as technologies and risks evolve.

Guide 2: Commitment to Responsibly Securing Emerging Technologies

This guide highlights practices that help cybersecurity professionals assess, communicate, and manage the security, privacy, and data risks associated with emerging technologies.

Practices to avoid

- Leaving emerging technology adoption unmanaged, allowing unapproved use to introduce significant security, privacy, and data risks.
- Sharing or uploading organizational data into unapproved public platforms or emerging technology tools.
- Assuming emerging technology tools are secure by default.
- Making emerging technology implementation decisions without alignment on security, privacy, data, and business risks.
- Responding to emerging technology risk with a blanket ban when a risk-managed, business-aligned solution is possible.
- Treating emerging technology outputs as authoritative when they may be incomplete, inaccurate, biased, or unsupported.
- Using emerging technologies to make high-impact decisions without appropriate oversight, human-in-the-loop review, or clear accountability.
- Overlooking vendor, contractual, or third-party risk when adopting emerging technology tools.

Reflection prompt: What are you already doing well, and based on these examples, what could you start, stop, continue, or change?

Guide 3: Commitment to Balancing Security and Business Objectives

This guide highlights practices that help cybersecurity professionals engage the business early, communicate risk clearly, and support informed decisions that balance security and business needs.

Effective practices

- Engage the business early to understand goals, initiatives, and desired outcomes so you can assess risk and help enable secure business decisions.
- Provide clear, straightforward guidance to stakeholders, including the laws, regulations, and standards that inform the decision.
- Collaborate with GRC and risk management partners to strengthen shared understanding of cyber risks and align with enterprise risk management.
- Ensure risk owners understand the full cost, effort, and operational impact of proposed risk treatment options.
- Create regular opportunities for cross-functional collaboration, including quarterly check-ins with cyber champions and business stakeholders, to keep security aligned with business activities.
- Consider the cost/benefit of recommended security controls, including their risk-reduction value and business impact.

Practices to avoid

- Overlooking regulatory or policy requirements for business convenience.
- Compromising long-term security for short-term business gains.
- Framing security solely as an IT or technology function.
- Relying on overly technical language or jargon when communicating with business leaders.
- Assuming risk is eliminated once a threat is addressed instead of reassessing likelihood, impact, and residual risk as conditions change.

Reflection prompt: What are you already doing well, and based on these examples, what could you start, stop, continue, or change?

Guide 4: Commitment to Responsible Use of Privileged Access

This guide highlights practices that help cybersecurity professionals manage privileged access with discipline, accountability, and appropriate oversight.

Effective practices

- Follow established access and security policies, and when exceptions arise, maintain transparency by consulting the appropriate stakeholders.
- Recognize the heightened responsibility and accountability that come with elevated access.
- Use privileged access management (PAM) practices to grant elevated access only when necessary and revoke it promptly when no longer needed.
- Ensure the organization has a structured approach to access provisioning and regular account reviews.
- Ensure privileged actions are logged in an auditable manner to support accountability and transparency.
- Follow the organization's change management processes when making changes to systems, access, or security configurations.
- Use just-in-time (JIT) access for privileged accounts to reduce standing privileges and the risk of compromise.
- Regularly review privileged access and privileged activity for compliance with security policies and approved use.

Practices to avoid

- Bypassing security controls, even when you have the ability to do so.
- Granting privileged access beyond the minimum necessary for a user's job responsibilities.
- Using shared privileged accounts where individual accountability and traceability are needed.
- Exempting administrators or other privileged users from the security standards, monitoring, and accountability requirements expected of all personnel.

Reflection prompt: What are you already doing well, and based on these examples, what could you start, stop, continue, or change?

Quick Self-Check: Applying the Code in Your Work

Use this quick self-check to reflect on how the Code shows up in your day-to-day work. It is meant to help you recognize what you are already doing well, spot areas where you may want to be more intentional, and decide which guide may be most useful to revisit.

For each statement, ask yourself: Is this true for me often, sometimes, or rarely/not yet?

Practice Area	Self-Assessment Rating
Security and Risk Reduction	
• I communicate security risks in ways the business can understand.	
• I help build a culture where security is a shared responsibility.	
• I look for practical ways to reduce risk while supporting business needs.	
Emerging Technologies	
• I consider security, privacy, and data risks when evaluating emerging technologies.	
• I help others understand the safeguards needed to use new technologies responsibly.	
• I raise concerns clearly so the business can make informed decisions.	
Balancing Security and Business Objectives	
• I engage with the business early to understand goals before recommending controls or requirements.	
• I explain risk in ways that support informed business decisions.	
• I look for solutions that protect the organization while enabling the business.	
Responsible Use of Privileged Access	
• I use elevated access only when it is necessary for my role or responsibilities.	
• I support accountability and transparency for privileged actions.	
• I follow access, logging, and change-management expectations consistently.	

Practice Guides:
What the Code Looks Like in Action

About ISC2

ISC2 is the world's leading member organization for cybersecurity professionals, driven by our vision of a safe and secure cyber world. Our more than 265,000 certified members, and associates, are a force for good, safeguarding the way we live. Our award-winning certifications – including cybersecurity's premier certification, the CISSP® – enable professionals to demonstrate their knowledge, skills and abilities at every stage of their careers. ISC2 strengthens the influence, diversity and vitality of the cybersecurity profession through advocacy, expertise and workforce empowerment that accelerates cyber safety and security in an interconnected world. Our charitable foundation, **The Center for Cyber Safety and Education**, helps create more access to cyber careers and educates those most vulnerable. Learn more, get involved or become an ISC2 Candidate to build your cyber career at **ISC2.org**. Connect with us on **X**, **Facebook** and **LinkedIn**.