Good approach	Poor approach
Evaluating risks	
You understand the risks suppliers may pose to your organisation and your wider supply chain. You are clear on the risks associated with their products and services.	You have a poor understanding of the risks that suppliers may pose to you and your wider supply chain. You don't understand the risks that come with their products and services.
You know the sensitivity of information your suppliers hold and the value of projects they're supporting.	You don't know the sensitivity of information your suppliers hold, and you don't know the value of the projects they're supporting.
Knowing the depth of your supply chain	
You know the full extent of your supply chain, including sub-contractors.	You only know your immediate suppliers and have limited or no knowledge of any sub-contractors.
Knowing your supply chain's security	
You know your suppliers' security arrangements and routinely confirm they're managing risks to your contract effectively.	You don't really know the security status of your supply chain, but you think it might be okay. You fail to review this status.
You exercise control over your supply chain and exercise your right to audit.	You exercise weak control over your supply chain, lose sight of sub-contracting, and fail to exercise audit rights.
An audit request would not be your first interaction with the supplier.	Often, your security team's first contact with the supplier will be an audit that follows an incident.
You may also require your suppliers to report on security performance, so your senior management team can be assured that all is working well	You don't require your suppliers to report on security performance. Your senior management team doesn't know how well or badly security is going.
Setting minimum security requirements	
Based on your assessment of risks and the security measures necessary to mitigate them, you set minimum security requirements for suppliers. You include your security expectations in your contracts.	You fail to set minimum security requirements, leaving it up to suppliers to do their own thing. (They might not have the security awareness to understand what measures are needed, or how to implement them effectively.) Or you set minimum security requirements, but fail to match them to your assessment of the risks — potentially making security unachievable for many of your suppliers.
Matching protection to risks	
You match the levels of protection required to the assessed risks and to the specific contract. You ensure these protections are justified, proportionate, and achievable.	You set a disproportionate 'one size fits all' approach for all suppliers, regardless of the contract and assessed risks. You fail to ensure these controls are justified and achievable — potentially putting suppliers off competing for contracts with you.
Managing security throughout the supply chain	

You expect your security requirements to be met throughout your supply chain. You check to ensure suppliers are complying.	You leave security to immediate suppliers to manage, but fail to mandate or check it is happening.
Meeting your responsibilities as a supplier	
You meet your own responsibilities as a supplier and challenge your customers for guidance where it's lacking.	You neglect your responsibilities as a supplier or ignore any absence of customer guidance.
You pass your customers' requirements down and report to senior management on security performance.	You fail to pass requirements down and fail to report to senior management on security performance.
Providing support in an incident	
You provide some guidance and support to suppliers responding to security incidents.	You offer no incident support to your suppliers.
You communicate lessons learnt so others in your supply chain avoid 'known problems'.	You fail to act or spot where 'known issues' might affect others in your supply chain, and to warn others about these issues. This lack of action potentially leads to greater disruption, with known issues hitting many suppliers.
Updating suppliers about changing cyber risks	
You tell your suppliers about emerging risks of cyber-attacks to improve their awareness. You actively share best practice to raise standards.	You expect suppliers to anticipate emerging cyber-attack risks and offer little or no support or advice, regardless of their security awareness and capabilities.
Building in assurance	
You build assurance measures into your minimum security requirements to give an independent view of the effectiveness of your suppliers' security. (Measures such as audits and penetration tests.)	You fail to include assurance measures in your security requirements. You believe your suppliers will do the right thing, regardless of whether they have enough knowledge or experience to know what is expected of them.
Monitoring the effectiveness of security	
You monitor the effectiveness of the security measures that are in place.	You fail to monitor the effectiveness of security measures.
You revise or remove controls that are ineffective based on lessons learnt from incidents, feedback from assurance activities, and feedback from suppliers about issues.	You fail to listen to feedback. You are unwilling to make changes, even when the evidence for doing so is overwhelming.