# Choosing a Service Delivery Model

Selecting the service delivery model that fits your organisation and delivers the required business and security outcomes is critical. Use the following SWOT (strengths, weaknesses, opportunities, threats) analysis to consider the advantages and disadvantages of the three most common models.

| | In-house | Procured | Hybrid |
|---|---|---|---|
| STRENGTHS | • In-house resources understand the business and the environment, and can make more business focused risk management decisions.<br>• Organisation has complete control of all relevant security policies, procedures and processes.<br>• Sensitive operational activities and information retained within the organisation. | • Supplier is responsible for recruiting, training and retaining security specialists.<br>• As a dedicated security organisation, the supplier is favourably positioned to hire and retain skilled resources, should have high security standards and be regularly audited.<br>• The supplier offers expert and specialist services as a core business. | • The supplier offers expert and specialist security analyst services as a core business.<br>• Supplier can provide critical friend and knowledge to help establish in-house service. |
| WEAKNESSES | • Visibility of the risk landscape beyond the boundaries of the organisation can be limited.<br>• Recruiting and retaining security specialists.<br>• Ongoing security specialist training commitment.<br>• With little or no experience of operating this type of service, it will take longer to establish a service and expose the organisation to increased risk. | • Business information and monitoring data will be held off-site and managed by the supplier, raising additional risks.<br>• Maintaining the continuity of archived records to meet legal or regulatory requirements when a contract is terminated. | • The need to recruit and retain some specialists.<br>• The need for some ongoing specialist training.<br>• Maintaining the continuity of archived records to meet legal or regulatory requirements when a contract is terminated.<br>• Some business information and monitoring data will be held off-site and managed by the supplier, raising additional risks. |
| OPPORTUNITIES | • Maximise investment in existing security products.<br>• Reduction or redeployment of security resources for greater effect.<br>• Development of in-house specialist security skills.<br>• Flexibility to change the security operations services as required, encouraging a more pro-active and dynamic risk management approach. | • More informed risk management capability as the supplier is developing analytic solutions to protect all its customers.<br>• The supplier should see patterns developing across their customer set, and provide advance warnings of attacks allowing defences to be put in place.<br>• The supplier may have existing 24/7 capability, if required.<br>• The supplier may provide mature incident response processes.<br>• Any dedicated security research capabilities within the supplier could benefit the organisation. | • Retention of sensitive operational activities and information within the business.<br>• Flexibility to tailor aspects of the service to meet specific risk management needs.<br>• 1st level response could be retained locally with the option to request support from external service providers.<br>• The supplier should see patterns developing across their customers that could provide advance warnings of an attack and allow defences to be put in place.<br>• Development of some in-house specialist security skills. |
| THREATS | • In-house security analysts may not see wide scale attacks developing.<br>• Easier for malicious insider to collude with in-house analyst.<br>• In-house service could be swamped by a major incident.<br>• Lack of skilled analyst resources in the market.<br>• The amount of information generated by the monitoring capability could flood the organisation. | • The supplier may be responsible for numerous customers and may time slice resources.<br>• The full business relevance of security events may not be understood.<br>• Not having an in-house capability may give a false sense of security, and affect the organisation's IA culture.<br>• The supplier may only offer a standardised service which may not directly support the organisation's risk management objectives.<br>• Reduced flexibility and increased risk, due to long lead times to deliver changes requested by the organisation. | • Blurring of in-house and supplier responsibilities, possibly leading to service delivery confusion (especially in the areas of incident response and handling).<br>• The supplier may be responsible for a number of customers and may time slice analytical and specialist resources. |



CESG