37th IAA SYMPOSIUM ON SPACE POLICY, REGULATIONS AND ECONOMICS (E3)
Space Sector's Commercial Transformation: Procurement Opportunities and Financial Transparency (6)

Author: Mr. Nils Holm Andersson
ESA, Sweden

SUPPLIER RISK MANAGEMENT IN PRIVATE AND PUBLIC ENTERPRISEES

Abstract

As the space sector increasingly embraces commercialization and private sector involvement, risk management becomes even more important to avoid mismanagement of resources.

Supplier Risk Management encompasses several risk aspects which are aimed at ensuring the buying companies operations, avoiding potential reputational damage and complying with increasing regulatory pressure as well as the wider publics expectations to act in a responsible way. Traditional risk such as financial and performance management is gradually expanded to include Sustainability/ESG risks, Cybersecurity, Climate or event risks (example location of producing sites in areas prone to earthquakes), and Compliance Risks including regulatory compliance.

A complete risk framework allows for a better understanding of potential areas of concerns and should be complemented with a set of tools for mitigating risks. For example;

1. Suppliers with low financial performance or high event risk due natural disasters should not necessarily be avoided if the commercial benefit is there. However, actions such as developing alternatives or having surplus stock if an event stops deliveries is crucial for these suppliers. An example of such an action is the current expansion of the semi-conductor industry into other geographical areas away from Taiwan due to the increase geopolitical risk.

2. A high sustainability risk for a specific geographical origin of the supplier does not necessarily exclude the supplier but requires mitigating actions. It also poses an opportunity to improve the supplier and delivery economic development for lower income countries. Example of mitigating actions is ethical audits, requirements on certification and participation in educational initiatives to reduce risk over time.

Note that practitioners should take a practical yet holistic approach to risk management and evolve the way they view risk over time. Cybersecurity risk is a good example where historically the risk has been viewed as only applicable for suppliers of IT equipment, software or other IT Services but is now transitioning to also include the risk of cyber attacks within key supplier supply chain.