

A hand in a dark blue sleeve points towards a central blue hexagon labeled 'RISK MANAGEMENT'. The background is a grid of hexagons, some of which contain text. The overall image has a blue and white color scheme with a blurred background of people.

# RISK MANAGEMENT

Avoid

Identify

Accept

Strategy

Reduce

Action  
plan

Transfer

Control

# 6 Steps for TPCRM

Mitigate

# 1 - Vendor Identification

Create a list of all vendors starting with those that provide important services or have access to sensitive data. Also take into account smaller vendors that provide support services.



# 2 - Risk Evaluation

Classify vendors based on inherent risk





### 3 - Use Questionnaires to Determine Residual Risk

Your organization may be required to comply with standards like ISO 27001, NIST SP 800-53, CSA CCM, etc. Your questionnaire should cover questions related to such frameworks and compliance requirements.



## 4 - Assign Ratings to Risks

Use a scorecard to determine the level of threat posed by the risks.

- High Risk - Deploy mitigation steps immediately
- Medium Risk - Deploy mitigation steps within a stipulated time frame
- Low Risk - Accept the risk or deploy mitigation steps over an extended period of time.





## 5 - Address Risks by Priority

Risks are mitigated based on importance & priority.

PRIORITIES





## 6 - Continuous Risk Monitoring

Risks are constantly changing and evolving and thus continuous monitoring is necessary.