Delegation of Security Functions in Organizations – Decision-Making Template

A. Organizational Scan (Detailed Survey)

It is important to understand how your organization works – its structure, culture, geography, history, risk management philosophy, etc… – to determine what, if any, part of the security program can be delegated downwards. The following factors should be reviewed:

Size: 0-50/ 50-500/ 500-1,000/ 1-2,000/ 2-5,000/ 5-10,000/ 10,000-20,000/ 20,000+

Geographic expansion: local/ regional/ national/ international

Employee composition: Full-time/ Part-time/ Locally-engaged/ Contractors/ Students/ Volunteers

Current policy framework regarding security issues: Policy/ Directive/ Standard/ Guidelines/ Guidance/ Other/ N/A

Organizational culture/orientation/focus: corporate/ operational/ technical/ security/ science/ compliance/ regional/ other

Trust/Risk Management Philosophy: Risk averse/ risk acceptable/ reasonable risk-takers/ unreasonable risk-takers/ reckless risk-takers

Senior management engagement: High/ Medium/ Low/ Unknown

Degree of security-related issues in the organization: High/ Medium/ Low/ None/ Unknown

- If any security-related issues, what is the public profile of these organizational issues: High/ Medium/ Low/ None/ Unknown

B. Security Risk Assessment (SRA)

It is then useful to conduct a baseline security risk assessment (SRA) to understand where security stands within the organization, how it is viewed and understood, what are the historical trends, etc… to aid in determining which functions could be considered for delegation/decentralization. Several options present themselves for such assessments:

Options:

- SRA conducted by a contracted resource (eg. external audit firm, specialist) Y / N
- SRA conducted by Internal Audit Y / N
- SRA conducted by yourself using information collected through:
  - Electronic Surveys Y / N
  - Paper Surveys Y / N
  - Focus Groups Y / N
  - Suggestion Box Y / N
  - Management-led sessions with canned questions Y / N
  - Sessions with Functional Communities (Managers’ Community, Regional Management Committees, EE committees, other committees, senior governance committees, etc…) Y / N

**Considerations:** If small and/or an all-local organization, then you should reach out and discuss face-to-face, use suggestion boxes and focus groups, even hire a specialist who can deliver this service in order to gauge the level of security penetration in the organization. Small organizations with regional offices can use a survey, regional focus groups, or an audit firm to determine how security is perceived. Medium organizations with a national footprint can use a combination of an audit firm, anonymous survey, and employee/management engagement across many fronts. Larger organizations can set up a project office with dedicated resources or casual employees with significant experience in the security discipline to conduct an in-depth review of how well security is anchored in the organization.

**C. Call to Action/Value Proposition**

*Once you have completed your baseline Security Risk Assessment, and before you embark on any major reorganization of such a foundational function as security, it is then wise to prepare a detailed call to action (or inaction as the case may be)/value proposition (or risk statement against moving forward) for delegation of security functions to subordinate organizations. A number of different considerations should form part of your case including:*

- SRA results (if available) Y / N
- Delegation of other similar programs within your organization Y / N
- Delegation within other similar organizations Y / N
- Examples of delegations (good or bad) ripped from the headlines if possible Y / N
- Impact of delegation if it goes wrong (impact on reputation, loss of confidence, impact on operations, political ramifications) Y / N
- Benefits of delegation (organizational flexibility, empowerment of local management, concentration on true strategic issues by national HQ security organization, partnership/inclusion of, and buy-in by, local management towards the success of the organization’s security program, etc…) Y / N
- Cost/benefit analysis (if possible) potential savings or efficiencies/costs to close the deal or counsel against it Y / N
Considerations:

You can build a strong case to justify or recommend against, as the case may be, the delegation of security functions to subordinate elements in your organization depending on: the level of senior management engagement and risk management appetite within the organization; the level of potential exposure that the delegation of security functions could bring to the organization; similar delegation efforts in parent organizations - both public and private; and public reaction to similar delegations gone wrong. However, it helps to point out that other departments/ agencies have done so already...

D. Policy Framework

The next step prior to considering any delegation of security functions to subordinate levels of the organization, is to assess the policy framework that directs and guides acceptable behaviours and activities within the organization. Consequently, you need to determine what type of security policy instruments, if any, exist within the organization and evaluate how current and complete they are. The typical security policy instruments include:

Options:

- Policy
- Directive
- Standard
- Guideline
- Guidance

<table>
<thead>
<tr>
<th>Policy Instrument</th>
<th>Yes/No</th>
<th>Date (if applicable)</th>
<th>Maturity (High/Medium/Low)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guideline</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guidance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Considerations:

Policy – generally strategic in scope, prescriptive and directive in nature, and cannot be interpreted to suit personal circumstances or styles.

Directive – amplify and drill down on narrower areas within the overall strategy, but still offer very little wiggle room.
**Standard** – very technical, “how-to” documents that are appropriate subordinate instruments to a higher-level policy or Directive, but still mandatory.

**Guidelines** – appropriate for organizations outside core public service that have different rules-set and work cultures/expectations, are not mandatory and can be interpreted to suit circumstances and preferences.

**Guidance** – appropriate for organizations that have no policy framework but who want to lay down a marker for future action, or a general statement of intent (eg. CEO’s Guidance on Security Program)

The more security delegation that is being considered within an organization, the more detailed and mature the policy framework underpinning the security program should be. Without constant oversight from the national HQ, it is more important than ever to have strong policy instruments for all security program elements that have been delegated to subordinate organizations.

### E. Detailed Risk Analysis of Security Program Elements

*It is then important to conduct a detailed risk analysis of all security program elements to determine which can be reasonably delegated to subordinate organizations and which must be maintained at the national HQ*

<table>
<thead>
<tr>
<th>Security Program Element</th>
<th>Element Maturity Level</th>
<th>Element Delegation Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Screening</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Awareness $ Training</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Event Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency Response Plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IM Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security in Contracts and Other Arrangements</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Considerations: The lower the maturity of the program element, the higher the delegation risk typically. Some exceptions apply, but as a rule of thumb, always err on the side of caution with security matters. You can always delegate more in the future as the subordinate organization improves its maturity level.

F. Detailed Analysis of Subordinate Elements of the Organization

The next step to consider is the maturity, capacity and/or ability of each subordinate organization to accept additional security responsibilities. Issues ranging from size, governance, location, and delegation of other similar responsibilities will help determine the suitability of each element to receive such delegation. It is quite possible and appropriate for some subordinate organizations to have greater delegation than others. Then an evaluation of each of the Security Program elements must be done to determine which elements can be delegated. There are generally three options for delegation of program elements.

Options:
- Full delegation
- Partial delegation
- No delegation

For each subordinate element, a maturity assessment needs to be done to determine suitability of dealing with delegated authorities.

<table>
<thead>
<tr>
<th>Subordinate organization Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factor</td>
</tr>
<tr>
<td>Security Governance</td>
</tr>
<tr>
<td>Geographic Size</td>
</tr>
<tr>
<td>Risk Management Philosophy (audit results)</td>
</tr>
<tr>
<td>Senior Management Engagement/Level</td>
</tr>
<tr>
<td>Security Culture</td>
</tr>
<tr>
<td>Policy Compliance</td>
</tr>
</tbody>
</table>

Overall Maturity Level Assessment:
Following the subordinate organization’s Maturity Level Assessment, the next step is to determine which, if any, Security Program elements to delegate to the subordinate organization.

<table>
<thead>
<tr>
<th>Subordinate organization:</th>
<th>Maturity Level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Program Element</td>
<td>Organizational Maturity Level</td>
</tr>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
</tr>
<tr>
<td>Security Screening</td>
<td></td>
</tr>
<tr>
<td>Security Awareness &amp; Training</td>
<td></td>
</tr>
<tr>
<td>Security Event Management</td>
<td></td>
</tr>
<tr>
<td>Emergency Response Plans</td>
<td></td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td></td>
</tr>
<tr>
<td>IM Security</td>
<td></td>
</tr>
<tr>
<td>IT Security</td>
<td></td>
</tr>
<tr>
<td>Security in Contracts and Other Arrangements</td>
<td></td>
</tr>
</tbody>
</table>

Considerations:

- **small sites with no organic security resources**: limited delegation to subordinate management, support provided from strategic-level HQ recommended
- **medium sites with some organic security and/or senior management on site (senior managers sub C-Suite level)**: partial delegation of such functions as physical security, emergency response, and BCP is recommended
- **large sites within a single country with significant organic security and senior management on site (C-Suite level equivalent)**: significant delegation to include most security program elements, including personnel security screening, security incident response, minus high-profile, consequential and complex investigations which should remain at strategic-level HQ.
- **worldwide sites that are part of large international organizations – maybe including many sub-sites - with full security complements and C-Suite leadership**: Complete delegation of operational tasks with few maintained at strategic-level HQ, but strong oversight function to monitor security program elements.
G.  Tools

Once a decision is made to delegate security functions to subordinate organizations, the next step is to determine which tools can be used to assist the subordinate organization in successfully implementing the delegated program elements. The first step is to determine which tools are available, then how they can assist the subordinate organization implement the security program element and, if applicable, how the organization’s strategic-level HQ Security team can use such tools to monitor compliance. There are numerous tools available, some of which are listed here:

- Strategically-focused note from CEO on Security culture and expectations – Sets Tone from the Top
- Organizational Security Policy Framework which clearly lays out in detail the expectations of senior management related to security
- Common look-and-feel BCP templates to ensure that local management has considered all issues in developing their business resumption plans
- Common look-and-feel Building Emergency Response Plans templates to ensure that all requirements are met
- Common emergency notification systems to ensure that security/EM issues are communicated in a timely fashion and that strategic-level HQ is aware
- Managers’ Self-Assessment of the Risk of Organizational Fraud, Waste and Abuse (FWA) to help detect the level of FWA risk
- 1-800 Information Hotline for confidential reporting and/or advice
- Managers’ Security Checklist (MSC) completed by head of subordinate organization to get a good read on the status of the security program at the local level
- Threat Risk Assessment Self-Audit Questionnaire including questions on all areas of security program (to be completed by all sites annually)
- On-line mandatory security awareness course with tracking to monitor who is aware of security procedures and requirements
- Security-related issue workshops with interactive voting technology provided by strategic-level HQ Security Team to dig deeper into local issues
- Code of Values and Ethics/Code of Conduct Annual Reminders to ensure employees are reminded of acceptable conduct
- Other tools developed by the strategic-level and local HQ Security Team

<table>
<thead>
<tr>
<th>Tool</th>
<th>Yes/No</th>
<th>Description</th>
<th>Strategic-level HQ Oversight Strategy (if appl)</th>
</tr>
</thead>
</table>
| 7/10
Considerations:

Any combination of the above tools can be utilized for any size organization. The more tools you provide to subordinate organizations to assist them in delivering the delegated program elements, the more confident they will become, and by extension the better you will be able to monitor compliance and performance, and adjust policies, programs and services to better assist them.

H. Verification/Compliance Strategy

The following step in the decision-making process is to determine which measures need to be in place to monitor, verify or otherwise confirm that the
security policy requirements are being met by the subordinate organizations. A variety of methods are available and include the following options:

- Detailed review of completed tools from the previous section:
  - Threat Risk/Physical Security Assessment Self-Audit Questionnaire
  - Common Bldg Emergency Response Plan and BCP templates
  - Managers’ Self-Assessment of the Risk of Organizational Fraud, Waste and Abuse
  - Records of Decision of local security governance/management committee meetings where security program elements are discussed
- Periodic on-site strategic-level HQ-Security Staff-Assistance-Visits (SAVs) to validate information provided in various reporting instruments
- Review of findings from Audits and other compliance activities where security may have been mentioned
- On-line surveys completed by security practitioners, managers and even employees
- Program Audits that include sampling from all levels, particularly if program elements have been delegated to subordinate organizations

Considerations:

Part of the decision to delegate program elements to subordinate organizations is the matter of trust. A past record of solid stewardship in other program areas (Finance, HR, OHS, etc…) helps to build the case for delegation. However, no matter the level of trust, due diligence requires verification of some form. The frequency and extent of that verification will vary based on the previous record of compliance and overall climate of trust.

I. Communications Strategy

The next step is to determine how to maintain close communications with the subordinate organization to ensure there are no questions and uncertainties related to expectations and boundaries within the delegation of security program elements. With the explosion of technology, there is a wide range of communications methods to stay in touch and maintain a trusted and supportive relationship with subordinate organizations. Some methods to maintain communications include:

- Video teleconference (VTC)
- E-mails
- Social media accounts (for non-classified stuff of course)
- Organizational classified network terminals for classified discussions
- Telephone conversations
- In-person meetings during Staff Assistance Visits or outreach activities
- Workshops to ensure that the local practitioners are completely aware and briefed on new responsibilities
- Structured training both in-house and with third-party service providers

**Considerations:** Early establishment of expectations and recourse mechanisms is vital when considering delegation of security functions to subordinate organizations. The initial discussions should be made in-person to ensure that there is a good rapport established between the national HQ element and the subordinate organization that is gaining new responsibilities. Periodic checks thereafter, by VTC, telephone, or drop-ins when traveling through the area, all maintain the confidence and trust of the subordinate organization in the parent organization and foster a climate of safe interaction when uncertainty exists.

**J. Feedback/Lessons-Learned Strategy**

*Finally, it is always important to remember the partnership and trust aspect implicit in delegation of responsibilities, where both sides feel safe to express themselves and acknowledge the need to be heard. Feedback is critical, as are lessons-learned. Some options to consider include:*

- Electronic surveys
- Paper-based surveys
- Suggestion box
- Structured Discussions with focus groups

**Considerations:**

Many of the same considerations elaborated in previous sections apply here. Depending on the size, geographic dispersion, demographic make-up of the workforce, and mandate of the organization, electronic surveys, paper-based surveys and/or suggestion boxes all may be applicable. What is essential is to hear from stakeholders at all levels to determine if there are program improvements that can be made, improved tools, guidance, etc… to ensure the organization’s security program is meeting its stated objectives.