Service Provider Resiliency Measures

Results of A Survey of EU Service Providers, Conducted for ENISA

Presented by IDC

About The Survey

- In order to examine the measures applied by network operators to ensure resiliency of their public eCommunication networks, ENISA requested IDC conduct a survey of network operators across the EU.
- Over two months in September and October 2008, IDC contacted close to 300 network operators in all EU member states.
- The objective was to interview senior managers responsible for ensuring network resiliency in as many operators as possible.
- IDC aimed to obtain a sample that included a wide variety of operators by geographic presence, size, network types, target market, and other variables.
- The full results will be published in the coming weeks in a study prepared by IDC for ENISA.
- This presentation summarizes some key results and highlights.

Survey Methodology

Because of the wide range of topics included in the survey, and the great variety of types of operators, multiple approaches were taken in conducting the survey.

- IDC collected most survey responses via telephone interview with individual managers responsible for network resiliency.
- In some cases, respondents collected information internally from multiple staff members, filling in the survey themselves and returning the completed questionnaires.
- Surveys were conducted in English or local language, depending on preference of the respondents.

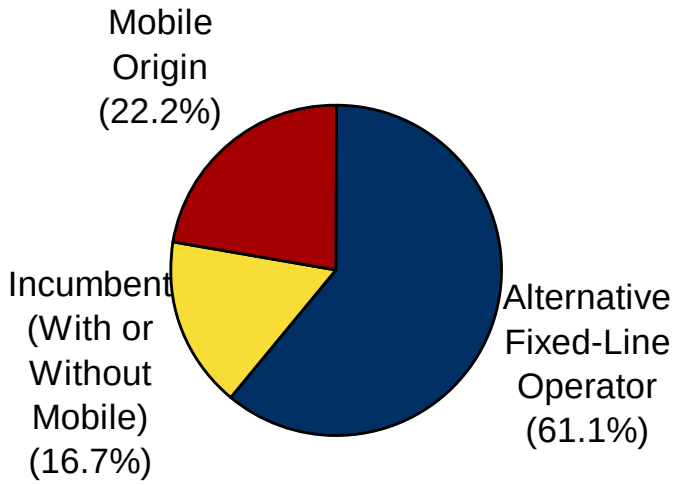
There were several challenges to conducting the survey. The most significant were:

- Reluctance of many operators to discuss what they considered to be sensitive security-related information with external observers
- Lack of standardization of terminology and organizational responsibilities around the issues of resiliency; virtually every company has different titles and division of responsibilities
- Because of the limited number of responses, one must be careful not to overstate the implications of the data

Summary of Respondents

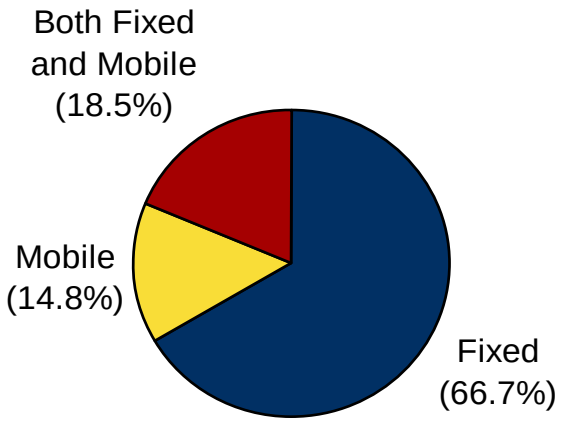
- Respondents were distributed across 17 of the 27 EU member states
- Wide distribution geographically, though a slightly higher proportion are from new member states
- Majority of respondents are alternative operators, usually much smaller than incumbents and mobile operators.
- With fewer incumbents and mobile operators in the market, there are fewer such respondents, though these tend to be very large.

Respondents by Type



Total=54

Respondents by Network Type

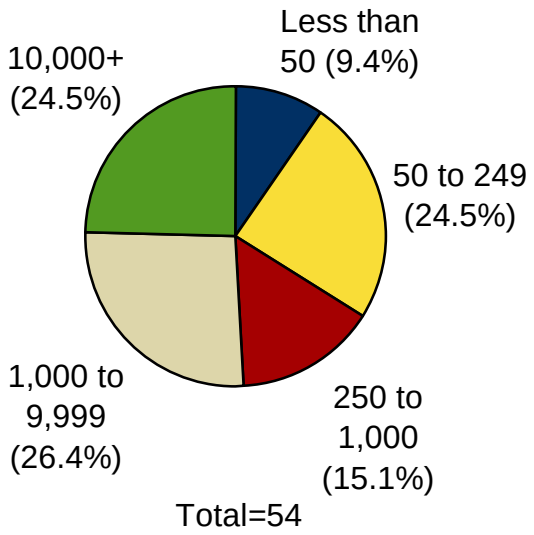


Total=54

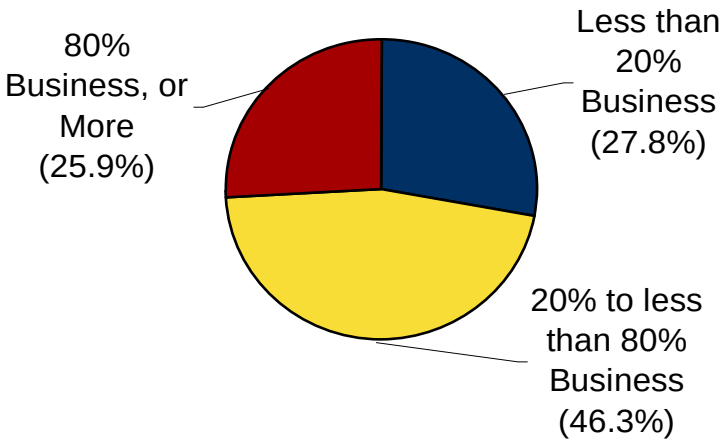
Summary of Respondents

- Respondents varied widely by size
- Most respondents targeted a mix of businesses and consumers, though just over a quarter each focused on business or consumer

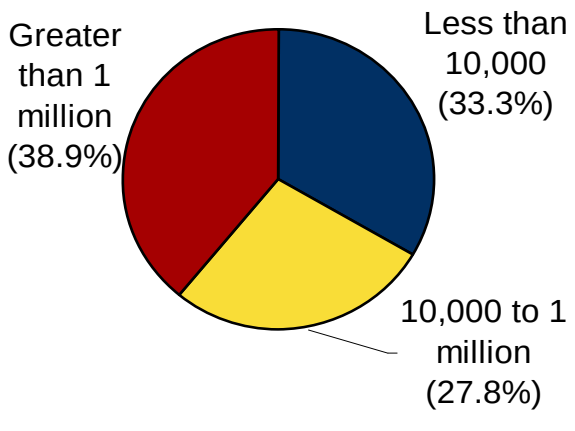
Respondents by Number of Employees



Respondents by Target Market



Respondents by Number of Subscribers

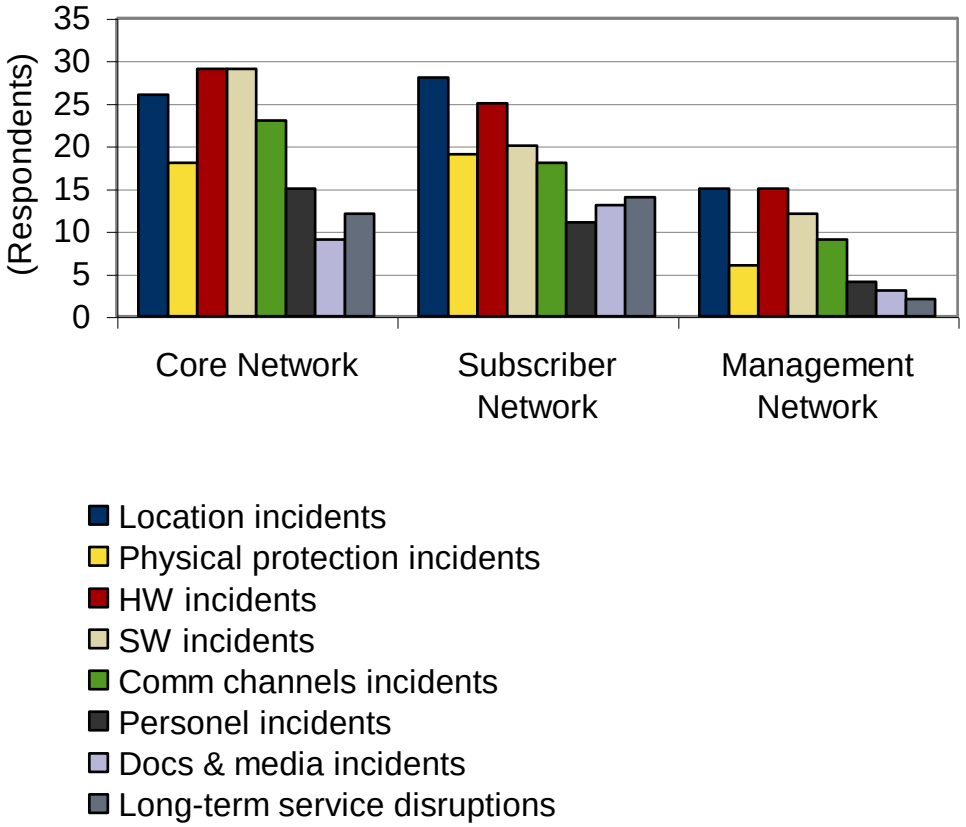


Threats to The Network

- Top threats to core network are hardware and software incidents
- Location incidents (e.g. fire) are also seen to be highly significant
- Threats differ slightly for subscriber networks, with location incidents most prominent
- Similar threats observed for management networks, though from fewer respondents
- Responses were generally consistent across segments, though mobile operators mentioned SW incidents in the core and long-term service disruptions due to unusually high demand more frequently than fixed operators

Leading Threats That Could Cause Network Outages

Q. What are the greatest threats that could cause outages in your network?



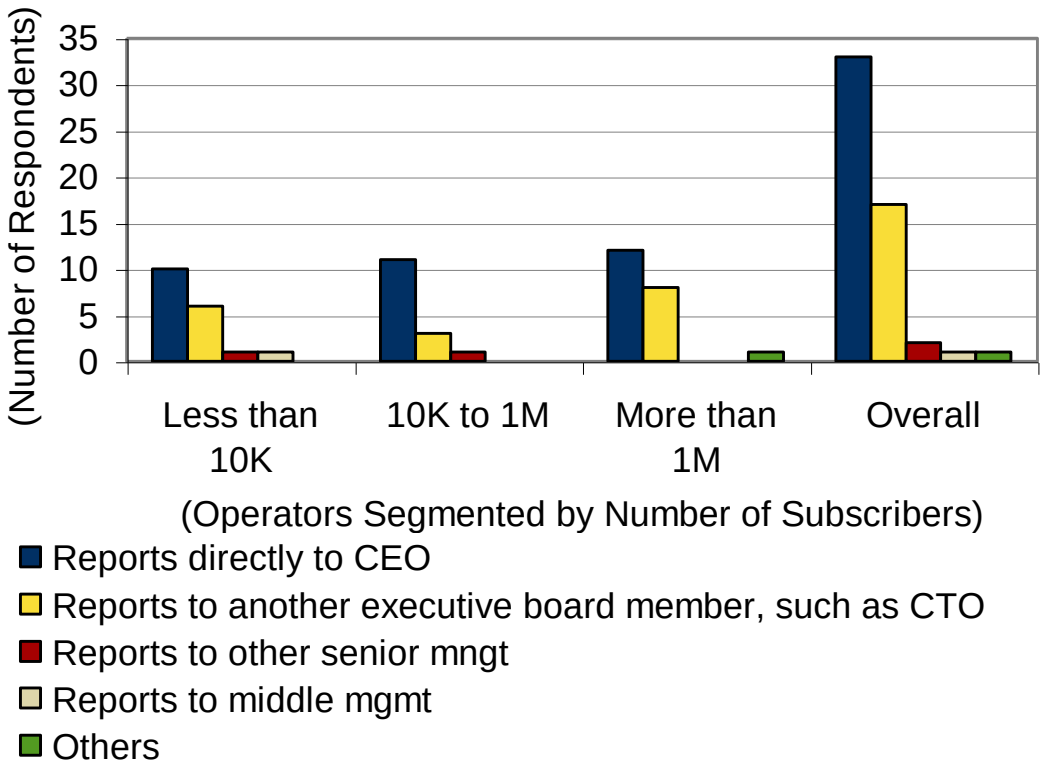
N=50

Organizational Factors

- Organizational structures and policies are an important aspect of addressing threats to network operations.
- In the survey, we aimed to identify how senior is the top employee responsible for network resiliency.
- Titles for this responsibility vary greatly, including such terms as CIO, Chief Security Officer, Emergency Coordinator, Business Continuity Coordinator, Corporate Risk Manager, and many other titles.
- Overall, the top resiliency managers almost always report directly to the CEO or to other top management
- There was little variation by segment

Seniority of Top Resiliency Manager by Size of Operator

Q. At what level is the most senior person responsible for ensuring network resiliency in the organization?



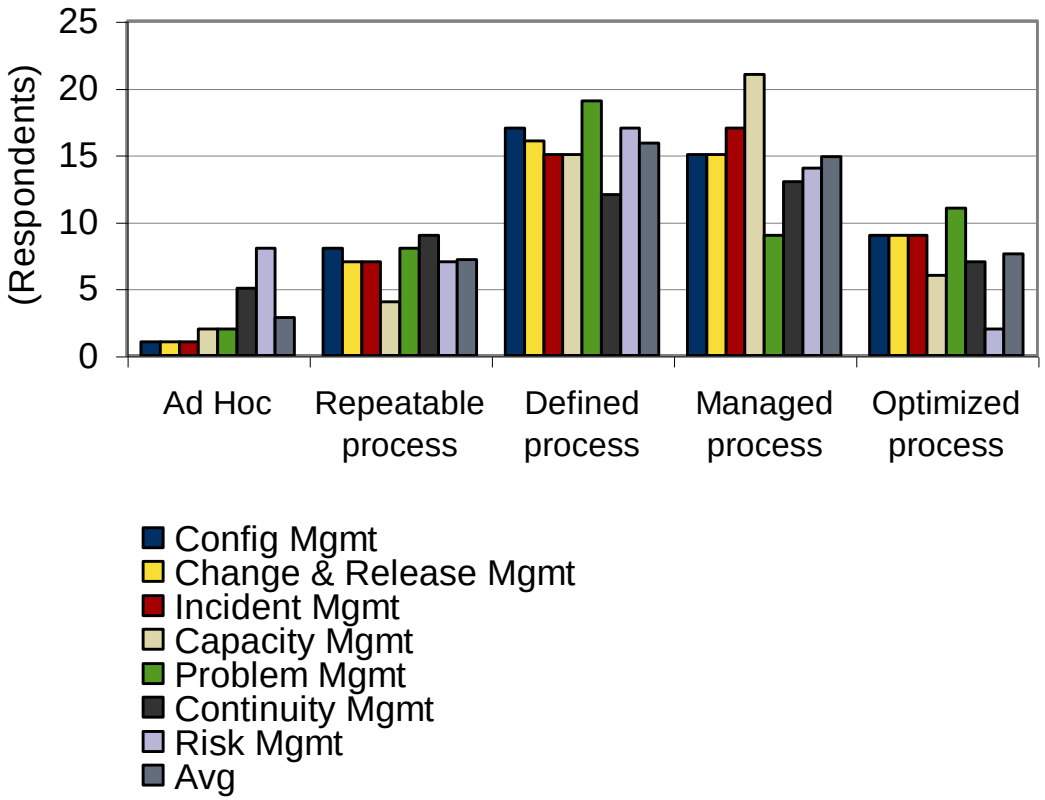
N=54

Maturity of Network Management Processes

- Operators must carefully address the development of network management procedures that help to avoid outages.
- Operators tend to describe their network management procedures as quite mature.
- Larger operators showed higher maturity levels of their processes.

Maturity of Network Management Processes

Q. Please describe the management processes that you use to manage the network?



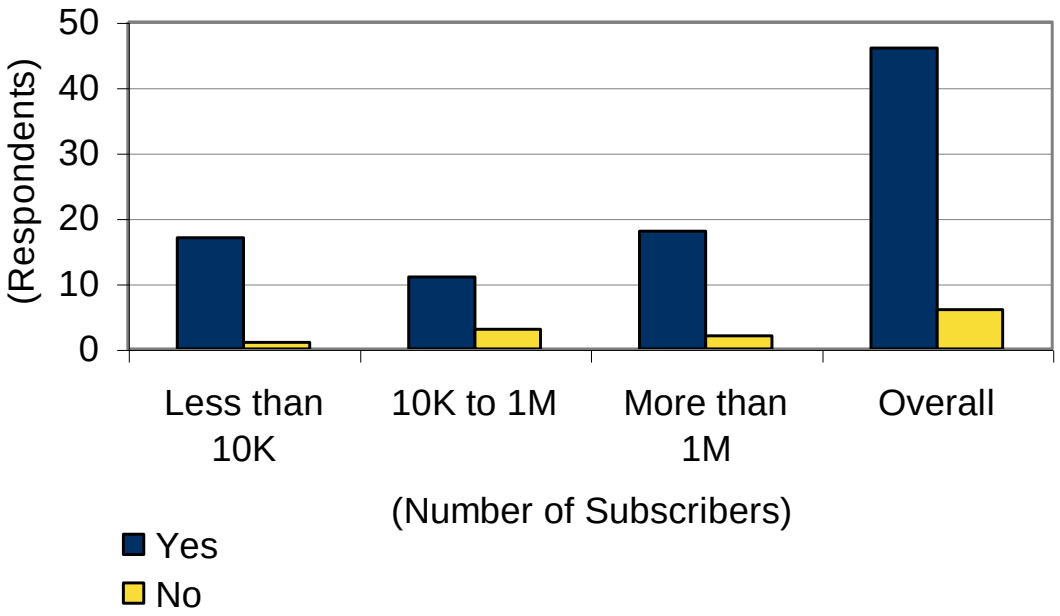
N=50

Business Continuity Measures

- In the event of network outages, it is critical that operators have effective business continuity procedures in place to ensure quick recovery from the outage.
- Most operators reported:
  - Using redundancy in the network to reconfigure in case of outage
  - And designing the network to minimize risk of single point of failure
- Most operators have defined business continuity procedures in place.
- Little variation by size, but almost all of those without such processes were Altnets.

Existence of Defined Business Continuity Procedures By Size of Operator

Q. Does your organization have in place some defined Business Continuity Procedures?



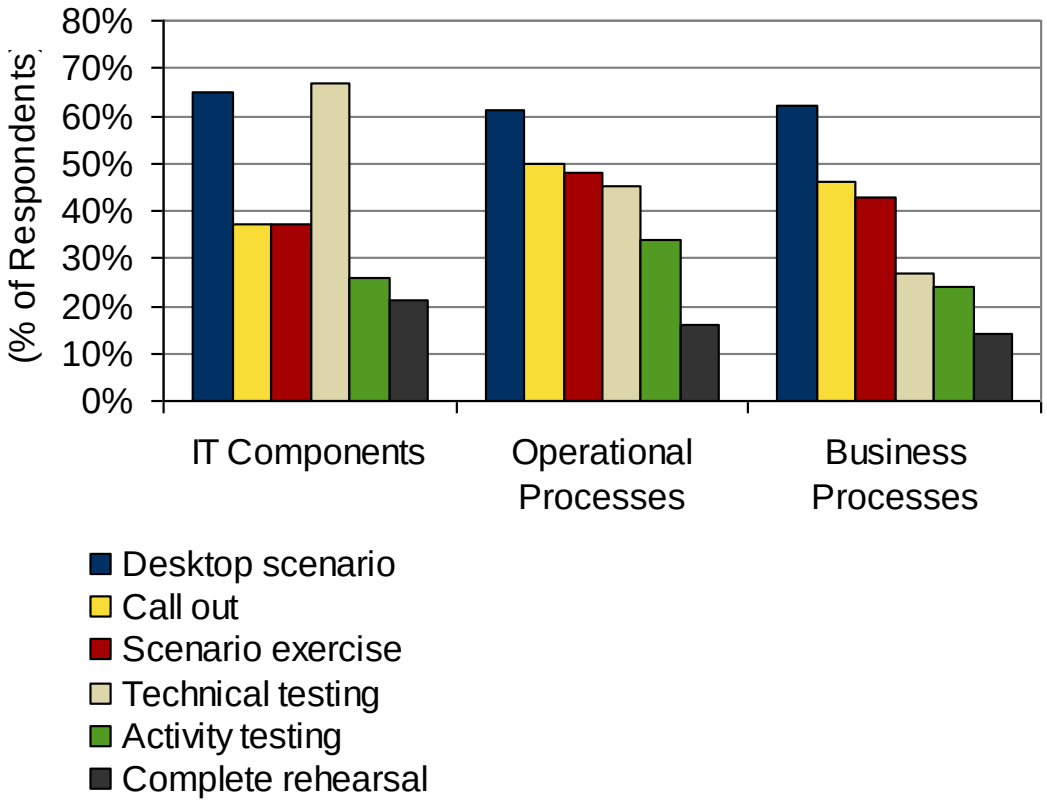
N=52

Tests of Business Continuity Measures

- There is a range of tests that can be performed to support and train staff on business continuity procedures.
- Two thirds of respondents conduct desktop scenarios, and technical tests are also common for IT.
- These tests are widely employed, though by no means universally.
- Different operators have different risk tolerances and resiliency challenges. But the industry and policy-makers may want to drive higher adoption of some tests.

Tests Performed in Support of Business Continuity Procedures

Q. Which types of tests, if any, are conducted in support of these procedures?



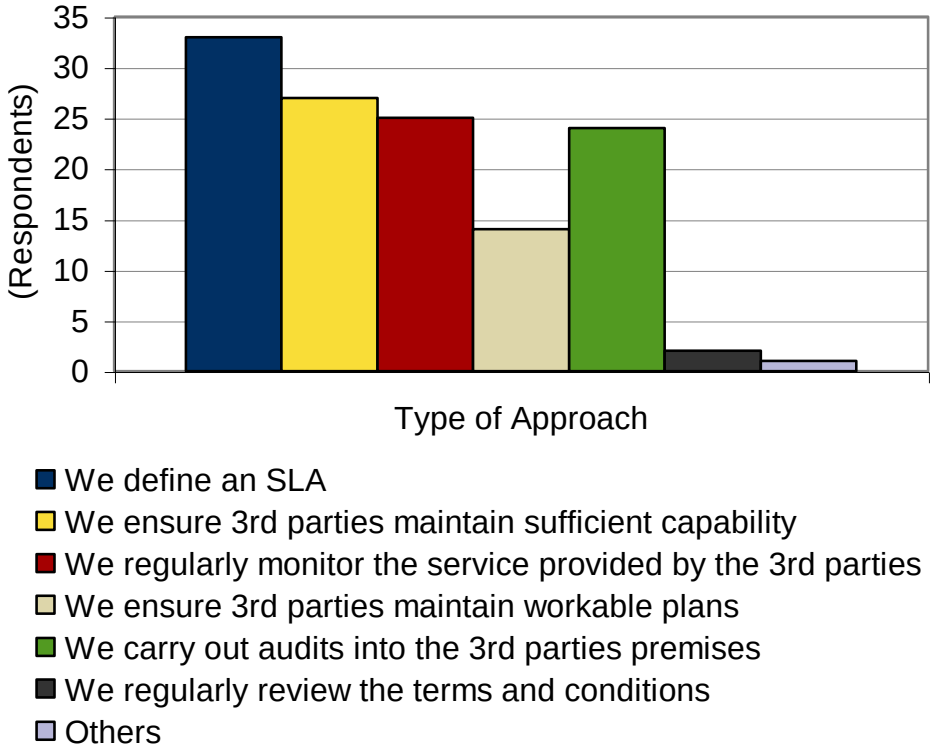
N=46, those having defined business continuity procedures in place

Third-Party Dependencies

- Third parties can bring resiliency threats that are harder to manage.
- Most respondents take some action to manage third-party dependencies–SLAs are most common,
- Higher adoption of measures to mitigate risks of third-party dependencies are probably needed.

Managing Third-Party Dependencies

Q. How do you manage the relationship with third parties?



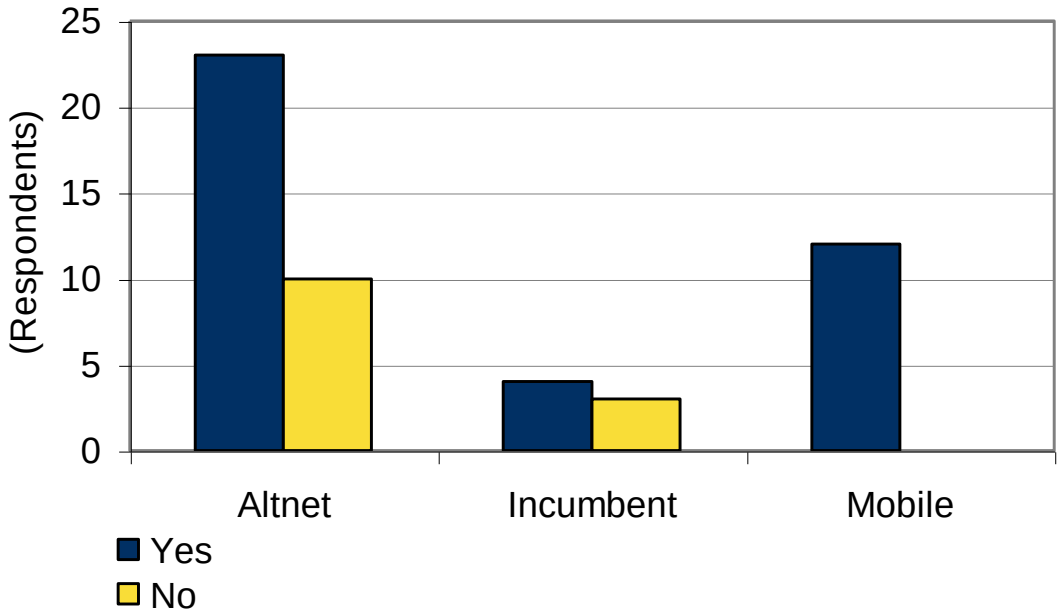
N=52

Third-Party Dependencies and Business Continuity Planning

- Most by not all respondents take 3rd-party dependencies into account in their Business Continuity Plans.
- All of the mobile operators took this into account.

Accounting for Inter-Infrastructure Dependencies in Business Continuity Planning

Q. Does your Business Continuity Plan take into account inter-infrastructure dependencies, such as dependency on 3rd party telecoms services or utilities?



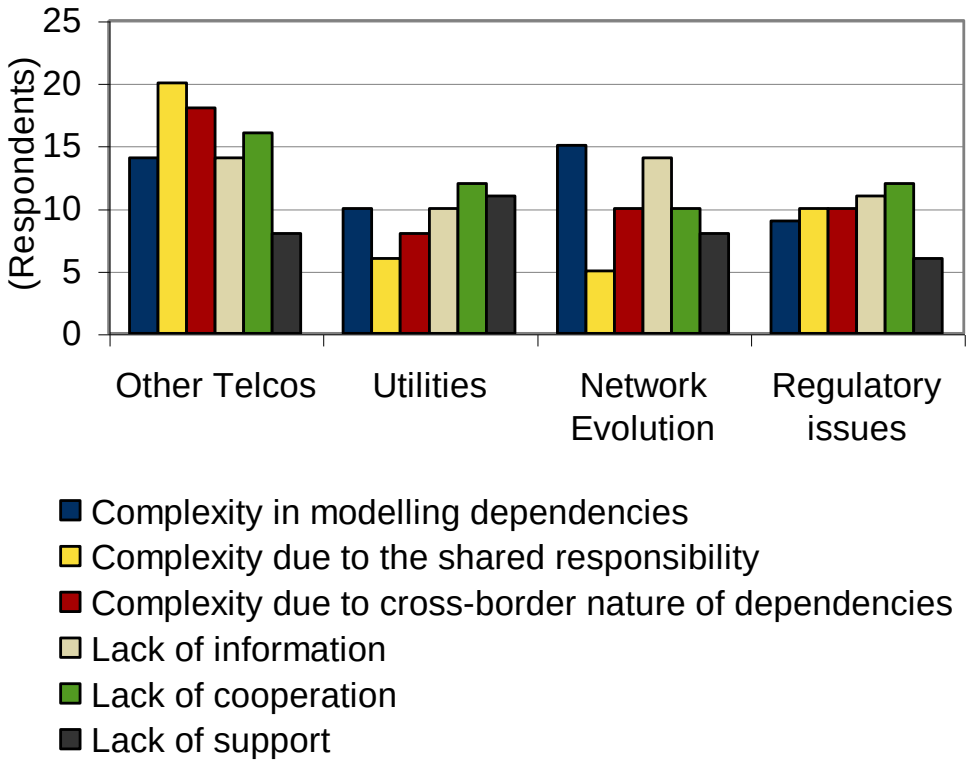
N=52

Challenges to Addressing Third-Party Dependencies

- Challenges in addressing third-party dependencies varied, depending on the partner.
  - With telecoms operators, complexity due to shared responsibility was most commonly cited.
  - With utilities, lack of cooperation was most common.
  - With regulatory issues, lack of cooperation was again most common.
- But generally, all issues were cited fairly frequently and should be addressed through greater industry cooperation.
- More sharing of experience and best practices in the industry would help greatly in this space.

Challenges to Dealing with Third-Party Dependencies in Business Continuity Planning

Q. When addressing inter-infrastructure dependencies, what are the main challenges?



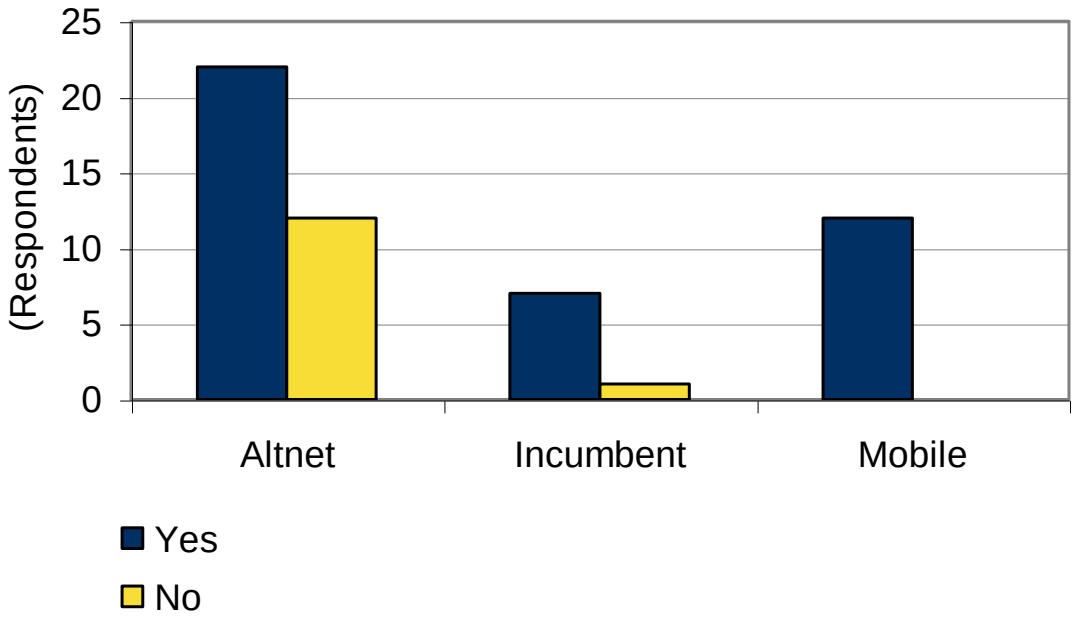
N=54

Risk Assessment and Management

- A significant number of respondents did not have processes in place to manage risks.
- Most of those without such processes were alternative operators.
- Because operators have different needs and risk tolerances, and because Altnets tend to be smaller with less complex management challenges, this may not indicate a problem.
- Nonetheless, IDC recommends further investigation of resiliency measures among Altnets, taking a closer look at their risk profiles and the degree to which their infrastructure is considered critical.

Existence of Risk Management Processes

Q. Do you have a process in place to assess and manage the risks pertinent to the businesses and services supported by your infrastructure?



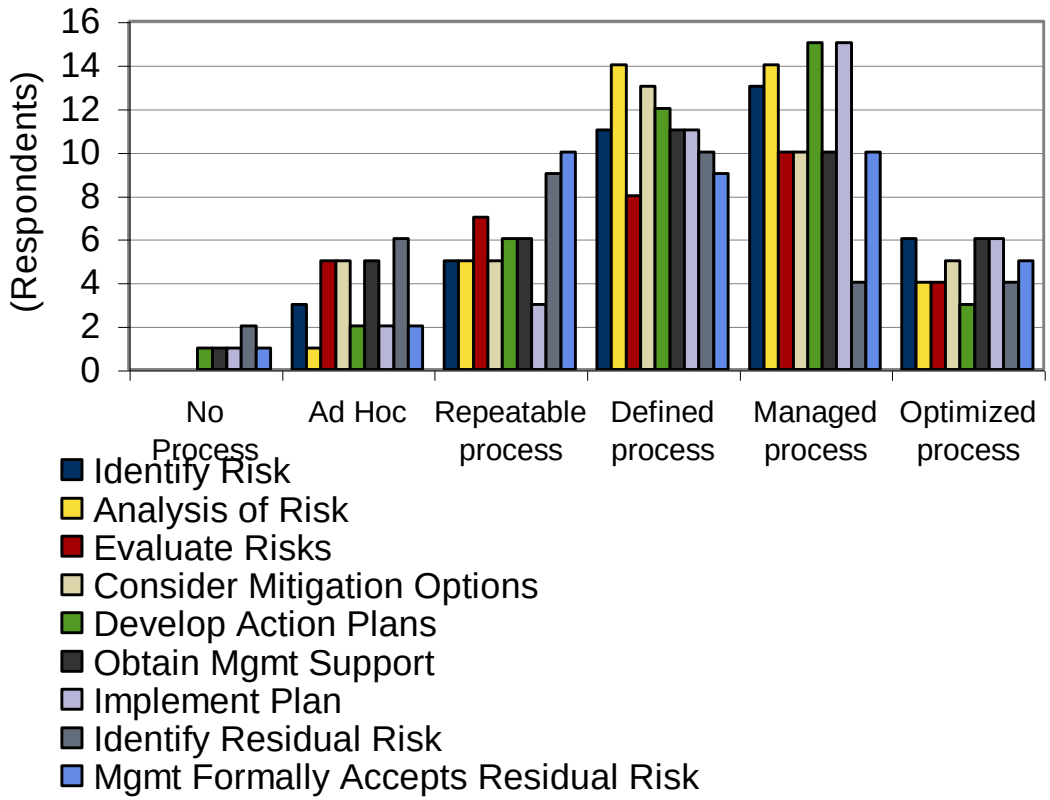
N=54

Maturity of Risk Management

- Of those that do have a process in place for risk management, these processes are generally quite mature.
- A small portion of respondents continue to manage this process in an ad hoc manner, but most use defined, managed or optimized processes.
- It is among Altnets where most of the less mature processes are reported. However, most Altnets did report mature processes.
- Taking into account those without any such processes in place, there is a significant portion of operators that may be subject to significant risks that they are not recognizing nor mitigating.

Maturity of Risk Management Procedures

Q. Please identify whether the following risk management processes are Ad Hoc, Repeatable, Defined, Managed or Optimized



N=39

Conclusions and Recommendations

- The survey indicates that most operators do take business continuity, risk management, and network resiliency very seriously. And many other operators refused to participate, due to the sensitivity of this topic
- Nonetheless, there are some weaknesses, especially:
  - Lack of critical processes in some operators
  - Immature processes in others
- As one might expect, it is among small alternative operators that many of the less mature processes are found.
  - That does suggest a need for further evaluation, and minimum standards.
  - But many of these operators are miniscule by comparison to the large operators on the market. Failure at one of these operators may not pose any significant threat to an economy or population.
  - Furthermore, some operators may have a business plan and service offerings that justify low effort on resiliency.
  - Nonetheless, IDC recommends further research in this area.

Conclusions and Recommendations

- Among large operators, substantial resiliency measures appear to be in effect. Some exceptions exist, and should be addressed, but the general picture is positive.
- Yet, the existence of processes and measures does not guarantee resiliency. Most operators appear to go it alone in this space, though many do seek support from external partners.
- Greater industry discussion is needed of the threats to networks and measures to mitigate them.
- The variation in types of operators, their business plans, their role in local markets, and their commitments to customers suggest that blanket policies are unlikely to be effective, at least not at this stage.
- IDC recommends the establishment of recommended guidelines or “best practices” that operators can measure themselves against and seek to apply.