The Quick Audit Tool

A help proposed by the CERL Security Working Group
in the fight against theft and vandalism

CERL Security Network

The Quick Audit Tool

Edition 1 - November 2018

Foreword

Collection security is one of the core concerns of the Consortium of European Research Libraries and an important area where we provide a service to our members by pooling knowledge and experience, sharing information about incidents in a confidential environment. We organize workshops, conferences and summer schools on collection security issues, and we will continue to explore innovative ways of addressing the security of our collections.

Based on the security survey which we created several years ago, the Quick Audit Tool created by Jacqueline Lambert of the KBR in Brussels, is an important new tool for us helping us to understand where we need to improve and how we can prioritize areas which may require investment.

On behalf of CERL I wish to express my gratitude to the KBR for enabling the work on this tool to progress so rapidly and I hope that the tool will prove useful for the very diverse membership of CERL
Kristian Jensen
Chair of CERL

I am really pleased to present this new tool "Quick Audit Tool" that is aimed to play a significant role in the support that the Security Network provides for the prevention of theft and vandalism. This first edition aims to offer a solid foundation for a set of tools which the Security Working Group plans to create, with the contribution of the Network. We hope it will help with translating the identification of issues into practical measures in the fight against theft and vandalism. My dearest wish is to see you convinced by this proposal and, thanks to your commitment to this project, to be able year after year to highlight and promote significant advances regarding strategies and practical measures developed to meet our primary objective.
Jacqueline Lambert
Chairman Security Working Group

Why we have developed the Quick Audit Tool

We have three main goals for our Quick Audit tool

First, we would like to raise awareness about the necessity for all institutions - from the smallest to the largest - to develop a policy to minimize the risk of theft and vandalism and to keep it constantly under review so that it remains effective. This policy includes the management of loss.

Second, we want to provide guidelines, so that those who are at the beginning of the process can have a good set of tools to meet this challenge and so that those who already have such a policy can ensure that all relevant aspects are taken into account, can assess their level of achievement compared with their peer institutions represented in the working group, and can find elements to improve their policy.

Third, through dynamic collaboration, we seek to provide the best possible support and to reduce the need for resource. We will do this by seeking to improve standards and to promote their use, by providing forms, procedures, check lists or other documentation. We will share experience on the use of equipment and on techniques and on any other theme relevant for prevention of theft and vandalism.

How we propose to meet our goals

The tool is based on a questionnaire which we have created to cover all topics relevant for the prevention of theft and vandalism.

The cumulated results derived from this questionnaire submitted by the participating institutions are aggregated in a form that will allow you quickly to establish a basic assessment / benchmark.

In addition, we provide concrete suggestions to help you to initiate, prioritize and coordinate your actions. Those are based on the one hand on the figures delivered by the survey and on the other hand on considerations specifically related to your institution. This means that small and large institutions can benefit equally from using the tool, as the outcomes can be adapted according to the available financial and human resources, etc.

In order to define both standards and best-practices (also relating to equipment and techniques), we aim to develop two supporting tools based on “one glance one click”. The process will include elements to support the sustainability of those tools. The results will only be accessible to CERL members.

Finally, we propose to undertake an annual review.

The aims of an annual review

Risk management requires a dynamic approach. The implemented policy needs to be continuously evaluated. It is necessary constantly to take into account internal or external changes affecting our institutions. Keeping up to date through an annual review reduces the risk that a security policy gradually loses its relevance.

Regular evaluation has the added benefit that it can act as a tool to reinforce the vigilance and the engagement of all participants.

Finally, this will allow the two practical tools to be kept under permanent review and to communicate their evolution to all CERL members.

The core: The questionnaire

Through around one hundred questions divided into six topics, the questionnaire aims to cover the aspects which are essential to meet the security needs of our collections and collection environment.

It results from a concerted exchange of ideas inside the CERL Security Network, with a special focus on the differing needs across the whole range of member libraries.

The questions are formulated so as to obtain the answers "yes", "no", "in part" or "not relevant". The answer "yes" is positive for collection security.

The topics addressed

Governance and policy

The questions addressed under this topic help to take stock of your institution's commitment to the fight against theft and vandalism. They highlight the necessity of working through a systems-based approach. They emphasize the need to stay vigilant and to be prepared to react promptly and appropriately in case of theft or vandalism, including near misses.

Collection management

The set of questions that you find under this topic aim to assess whether, from a practical point of view, you have the necessary tools for the reliable identification and monitoring of your collections, for keeping a constant vigilance and being able to provide increased vigilance and protection for highly valuable/vulnerable items.

Physical security

The questions addressed under this topic are intended to guide you in securing the building: from the external perimeter to the reading rooms and storage areas. They are also intended to ensure the adoption of

procedures necessary for access control, including responsiveness in the event of an incident.

Access and use

The questions addressed in this section are intended to guide you in the adoption of rules about access to collections and their use both by readers and by members of staff. The problem is approached from several angles: limiting the access to storage and proceeding areas, the ability to track all the collections items, specific rules for high valuable/vulnerable items, and constant and varied vigilance including measures of deterrence in reading rooms. This requires regular monitoring and rigorous adherence to the rules, including limitations on access. Staff awareness and buy-in is essential for this.

Exhibition and transport

The set of questions that you find under this topic aim to tackle risks specifically inherent in transport and exhibitions. All new environments require assessment for us to be able to manage risks, and this requires special expertise. Issues of physical protection during transport are integral also to collection security. The conditions and the invigilation of temporary or new exhibition areas have to be adapted to the displayed items, etc. Relationship issues can arise because third parties have to comply with specific rules and standards.

The unusual & crises

This last topic is dedicated to situations beyond common /customary/ ordinary work with the collections. Whether it concerns an intervention following a disaster or a technical intervention in a storage area, it's important to be exceptionally vigilant to keep control on access to the affected collection items, to track them and to avoid or minimize inappropriate handling that could result in damage. In this case, too, third parties will be subjected to rules and standards.

The resulting standard for basic assessment / positioning

All institutions represented within the Security Network working group were asked to answer the questionnaire. The results were processed and transcribed in a document composed by as many tables as there are topics.

In addition to the title line, each table consists of as many rows as there are questions covering the theme and it consists of five columns. The first column has the number of the question, the second the percentage of institutions which responded "yes", the third the percentage of institutions which responded "no", the fourth the percentage of institutions which responded "in part" and the fifth the percentage of institutions which have responded "not relevant".

This document represents the starting point for your assessment / positioning exercise.

Next, you are invited to highlight the column corresponding to the answer given by your institution with the following color code: green for yes, red for no and orange for in part.

As a result, at a simple glance you get clear first visualization of your situation.

How to initiate, prioritize and coordinate actions

The proposed procedure will highlight your situation (see above) and is a first help to highlight topics where there is room for improvement, and to get an initial idea of the problems you have to tackle.

But, it would be wrong to focus only on the questions for which you answered "no" or "in part". The questions answered positively also require analysis. Were you sufficiently critical when you answered? Are the existing solutions mature enough or really efficient? We have a duty to question some "confirmed" solutions.

When dealing with questions where you answered "in part" you can analyse the reason for incompletion, determine if the partial solution suffers from a lack of harmonization, or, perhaps more difficult to admit, that you cannot apply a rule more broadly because it is inadequate or inappropriate.

At a certain moment, it becomes healthy to accept errors and failures. Being able to admit omissions and problems is essential to succeed. It is better to take a step back, to rethink things than to persist in what is doomed to fail.

The figures mentioned in the "standard" represent a significant help: a rule implemented within 80% of the representative institutions is likely either not too hard or crucial too to implement, whereas a rule implemented by only 20% of the institutions, could either have a lower priority or be really hard to achieve.

Referring to the standard can induce a real dynamic; it offers an opportunity to boost projects concerning security of the collections. Positioning in relation to peers will inevitably have an emulation effect. It's also a valuable source for articulating the importance of specific activities.

For all the points / problems to which you want to bring solutions you first have to determine a) the over-all context, including obstacles and dependencies on other activities that may have an impact on security measures, b) the implementation, and c) the sustainability of your security measures and what factors play a role in this sustainability. These inevitably vary from one institution to another and can have an impact on the prioritization and the extent of measures. With that in mind, opting for less

ambitious but sustainable measures is preferable to adopting measures that cannot be properly achieved and/or sustained.

Any decrease in term of risks has to be considered as a victory, so do not undervalue small actions. Rome was not built in one day.

Hereafter some elements to take into account before embarking on the concretisation of any solution / measure.

Is the achievement 100% within your control or not? What about the degree of difficulty, the cost? Do you have the expertise within your institution? All this can substantially impact a schedule. It is important to be able to assess the time needed for the implementation of a solution/measure, and to be sure that the means at your disposal, whether in terms of budget or staff, are sufficient. This helps you avoid choosing inappropriate solutions/measures or making premature launches which could weaken any solution/measure, however good it may be.

Psychological aspects must not be neglected either. What about possible internal obstacles? How do you ensure buy-in and adherence to new measures?

It is important to involve as soon as possible, in one way or another, all who may be concerned /affected. That is also a way of getting an accurate idea about what already exits and works. This can be really valuable to avoiding loosing precious time.

Plan time to raise awareness, to ensure that everybody understands what is going on. Providing training in the proper use of all the measures is essential. If staff understand the rules and feel comfortable and confident with them they are more likely to comply with rules.

Don't forget the basics. For example: without knowledge of your building it's impossible to protect it. It is for instance an essential prerequisite to have plans with basic elements of your infrastructure such as a numbering system to identify individual spaces, as well as the lay-out of shelves in the stacks with their numbering.

Coordination with other related policies will optimize your approach to all types of risks.Linking the safeguarding of the collections with the general Security and Health and Safety (or similar) policies provides you with coherence in terms of risk management. Such coordination also has the potential for enhancing separate policies which have similar objectives: looking for maximum protection through optimal prevention and developing the ability to deal with the unforeseen, from mini-crisis to disaster.

They have similar needs, reliable documentation, basic facilities and devices and last but not least, adherence and participation of staff including the highest level of the organization.

The approach is similar, namely the dynamic risk management through knowledge of both the environment and the human factor.

The interaction between the different risks is obvious. Let's take an example. Good housekeeping is necessary to guarantee evacuation, intervention from the emergency services, and even cleaning, which is important to avoid infestation and mold. It also helps with spotting anomalies in the storage areas or where collections are used.

In this way collection security policies can enhance legal compliance with health and safety regulations and with fire protection rules for instance while it can at the same time benefit from being integral to policies which are legal requirements.

Supporting tools

Beyond helping you to take stock and to plan and/or refine measures, we also intend to bring you more concrete support.

We feel that many of the resources which are available on-line often require a lot of time, before anything concrete can be derived from them. They also tend to reinforce each institution working in isolation. At a time when many institutions face budgetary challenges, where staff have to concentrate on tasks that bring visible results, we would like to leverage collaboration within the network to create two practical tools.

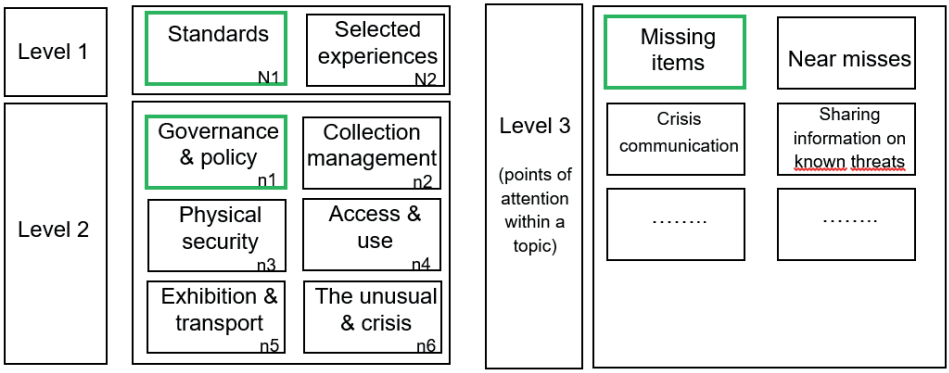
The first tool would be dedicated to standards (forms, procedures, check lists…) and the second one to the sharing of selected experiences in all relevant areas (equipment, techniques….).

Concept

Both tools would have a similar approach and presentation.

Our initial thoughts are to lead the user through an interactive file / interface that has four levels:

- Level 1: would give you the choice between standards & selected experiences
- Level 2: would give you the choice between the 6 topics of the questionnaire
- Level 3: would allow you to choose a point of attention within your chosen topic
- Level 4: would list a relevant set of documents concerning the chosen point of attention. The list will take into account the differing needs across the whole range of member libraries



N/n=number of items at disposal N1= $\sum_{i=1}^{6} ni$

Level 4

(list of relevant resources)

Governance & policy Missing items			Standards	
Size of the institution	Internal statement		Reporting to the police	
	procedure	form		
Small	Example 1	Example 1		
Medium	Example 2			
Large	Example 3			

Implementation

This first edition of the Quick Audit Tool launches the process of developing the supporting tools.

The development is based on a dynamic collaboration. With the help of the Network, in several stages, the Security Working Group aims to collect a maximum of information and examples. Then, the Security Working Group will categorise the information, guidelines, tools and examples that come it. After the information is thus structured, it will be made available to CERL members. Over the years, the information is added to, enhanced and kept up to date.

Target for the first year

Our first step is to formulate a request to members of the network to send information and examples to the group and to assess and process the information thus received. In this first stage we hope to bring together 50 relevant items. Secondly, we will develop the 4 levels interactive interface that will give access to the documents made available thanks to this dynamic collaboration.

Finally, this first set of relevant information would be advertised in the second edition of the QAT.

Annex 1: the Questionnaire

	Governance & Policy
1	Your mission statement expresses a commitment to ensuring the security of your collection
2	Your most senior member of staff (e.g. Director, Chief Executive) has final accountability for the security of your collection
3	An annual report on the security of your collection is presented to your governing body
4	You have a Collection Security Policy (or set of policies) that sets out how you protect your collection
5	You have an agreed set of measures to provide assurance on the security of your collection and to assess compliance with your Collection Security Policy
6	Your Collection Security Policy also covers your digital collections
7	Staff with authority for policies relating to the collection, including its management , storage, use, exhibition, conservation and transport, have input into the Collection Security Policy
8	Your policies and written procedures, including any sanctions that you apply are understood to meet the legal requirements and are enforceable
9	You have an agreed written procedure for investigating, handling and documenting missing collection items
10	You have an agreed written procedure that details how you respond to instances and near misses of theft and mutilation/vandalism
11	You immediately report proven instances of theft and mutilation/ vandalism to the police
12	You report proven instances of theft to relevant trade/professional bodies - e.g. the book trade
13	You share information on known threats to collection security with other libraries/archives when appropriate
14	You have procedures in place for crisis management, including crisis communication
15	Your collection security policies and procedures are kept under regular review

	Collection Management
16	Collection security is taken into consideration in all collection management procedures
17	You maintain catalogue records for your collection
18	You include copy specific information, such as the presence of bookplates or inserted maps, in new or enhanced catalogue records for heritage materials
19	You create and retain accession records for acquisitions that are especially valuable, vulnerable or controversial
20	You maintain knowledge of the physical features that characterise materials in your collection, such as typical ownership marks and typical binding styles
21	You place ownership marks in your collection items
22	You place shelf mark labels on your collections items where appropriate
23	You assess the security requirements of collection items, so that highly valuable/vulnerable items are identified and given increased protection
24	You have an agreed and documented disposals policy: disposed items have a clear cancellation stamp in them
25	You have measures in place to prevent unauthorised changes to your accession and catalogues records
26	Readers are encouraged to use digital or microform facsimiles of heritage materials that are especially valuable or vulnerable, except where there is an approved research reason for consulting the original
27	You audit / check your collection in the stacks to provide assurance on its security
28	You make and retain copies of high value items
29	Where a high resolution copy of a rare or vulnerable item exists, this will be used to generate further copies in place of the original item
30	Your collection is insured (if permissible) or the State acts as its own insurer

	Physical Security
31	All points of access to your building(s) can be secured
32	You have a security presence in your building 24/7
33	Your security staff comply with nationally recognised professional codes
34	Response to the activation of the alarm system is within 2-5 minutes
35	There is CCTV coverage of the Reading Room areas where highly valuable/vulnerable items are used
36	CCTV covers all entrances, exits (including emergency exits) and service routes
37	CCTV records are retained in accordance with legal requirements
38	There is an effective security barrier between the public parts of your building(s) and staff offices/storage areas, to prevent unauthorised access to restricted areas
39	Security staff are consulted on proposed building alterations as early as possible in the process and certainly prior to work commencement
40	Access to keys is strictly controlled
41	All keys are returned to a central, secure location at the end of the day for logging and storage
42	Electronic access is used wherever possible
43	Electronic access systems, if in place, are reviewed regularly
44	A designated member of staff (or deputy) can be contacted at any time out of hours in the event of a security incident.
	Access & Use
45	Readers may only access your collection if they undertake to comply with your Reading Room rules and regulations
46	You gather sufficient information about your readers to be confident about their identity and would be able to contact them in the event of a security investigation
47	You retain essential identity and contact information about your readers for as long as permitted or justifiable within the law

48	Readers are not permitted to bring coats or large bags into your special collections reading room(s), nor any object that might harm the collection (e.g. knives, blades, food, drink)
49	Readers' belongings are searched as they exit the Reading Room
50	You have agreed procedures for the use of uncatalogued items: this includes close invigilation by staff
51	Readers' use of highly valuable/vulnerable items is invigilated by staff
52	You limit the number of items that may be seen at any one time by a reader
53	Highly valuable/vulnerable collection items are inspected by staff before and after use
54	Highly valuable/vulnerable collection items are weighed before and after use
55	You have procedures in place for the use of material with restricted access
56	If legally permitted to do so, you permanently retain a record of collection use allowing you to identify the items used by each reader, and to list all users of a particular item
57	Readers cannot gain access to areas where heritage materials are stored, unless escorted by authorised staff
58	Readers cannot gain access to areas where heritage materials are processed (e.g. conservation, reprographics), unless escorted by authorised staff
59	Staff must be authorised to access collection storage areas
60	Staff access to collection storage areas is restricted on the basis of need
61	Staff access to collection storage areas is reviewed on a regular basis
62	The number of staff able to access Strong Room is strictly controlled
63	You have an agreed policy on the maximum time that staff may retain collection items
64	Procedures are in place with respect to staff taking collection items offsite for personal use
65	Police checks and/or personal references are obtained for everyone in your organisation (including staff, contractors, interns and volunteers) before they are permitted to start work

66	Information on your Collection Security policy is given to all new staff as part of their induction training
67	Awareness training is delivered regularly to staff to ensure that they remain aware of their responsibility for collection security
68	You maintain a complete record of all collection items consulted or processed by individual members of staff for as long as permitted or justifiable within the law
69	Staff and departments that routinely use collection items are audited regularly to assess their compliance with your collection security policies
70	Staff at all levels of your institution are required to comply with your collection security policy
71	Staff whose work involves contact with the collection have their collection security responsibilities included in their job descriptions / role profiles
72	You reserve the right to inspect staff belongings as they leave the building(s)
73	All staff and authorised visitors to office and storage areas are immediately recognisable as such (e.g. by wearing a visible ID card or visitor pass)
74	All staff must use agreed procedures for retrieving items for their personal use
	Exhibition & Transport
75	You carry out condition reports on collection items before and after they are exhibited; this may include a photographic record for items loaned to other institutions
76	You display collection items in secure, alarmed cases
77	Exhibition areas are patrolled by staff or security personnel during open hours
78	The condition of displayed items is checked regularly while on display
79	The condition of displayed items of high value is checked daily
80	The condition of displayed items is checked before (during) and after exposure

81	You provide training to staff who act as couriers when taking items to other institutions
82	You require all request for loans to be accompanied by a facility report on the borrowing institution
83	You agree formal, legally binding loan contracts with institutions to which you lend items; these specify the conditions under which the items will be lent and exhibited
84	A financial valuation is prepared for all exhibited items
85	Items are insured when exhibited at another institution
86	You have staff with specialist training in packing collection items
87	You use specialist removal contractors to transport items
88	Collection items transported to and from exhibitions are accompanied by a courier
89	You have an agreed procedure for the transport of items within your building
90	You have an agreed procedure for the transport of items between your buildings (if relevant)
	Unusual & Crisis
91	Unauthorised personnel are escorted whilst in the collection storage areas, by Library staff.
92	Collection security information is given to all new personnel and contractors as part of induction training
93	Staff, contractors and visitors to non-public areas, must be identifiable e.g. by wearing ID badges or visitor passes
94	You have an agreed procedure for carrying out large scale book moves
95	You have an agreed procedure to ensure the traceability of collection items moved during crisis management
96	You have procedures to prevent as far as possible the mutilation of collection items during crisis management

CERL SWG : "Resulting Standard" QAT version 2018

Governance & Policy	yes	no	in part	N. R.
1	54,55	18,18	27,27	0,00
2	90,91	0,00	9,09	0,00
3	36,36	45,45	18,18	0,00
4	81,82	9,09	9,09	0,00
5	72,73	9,09	18,18	0,00
6	45,45	18,18	36,36	0,00
7	72,73	9,09	18,18	0,00
8	72,73	9,09	18,18	0,00
9	45,45	36,36	18,18	0,00
10	45,45	27,27	27,27	0,00
11	72,73	0,00	27,27	0,00
12	54,55	0,00	45,45	0,00
13	81,82	0,00	18,18	0,00
14	90,91	0,00	9,09	0,00
15	72,73	9,09	18,18	0,00

Collection Management	yes	no	in part	N. R.
16	81,82	0,00	18,18	0,00
17	90,91	0,00	9,09	0,00
18	45,45	0,00	54,55	0,00
19	90,91	0,00	9,09	0,00
20	54,55	0,00	45,45	0,00
21	63,64	0,00	36,36	0,00
22	90,91	0,00	9,09	0,00
23	63,64	0,00	36,36	0,00
24	81,82	0,00	0,00	18,18
25	63,64	9,09	27,27	0,00
26	63,64	0,00	36,36	0,00
27	36,36	0,00	63,64	0,00
28	36,36	9,09	54,55	0,00
29	72,73	9,09	18,18	0,00
30	63,64	36,36	0,00	0,00

Physical Security	yes	no	in part	N. R.
31	100,00	0,00	0,00	0,00
32	63,64	9,09	27,27	0,00
33	90,91	0,00	0,00	9,09
34	81,82	9,09	9,09	0,00
35	81,82	0,00	9,09	9,09
36	36,36	18,18	36,36	9,09
37	81,82	0,00	9,09	9,09
38	54,55	9,09	36,36	0,00
39	72,73	0,00	27,27	0,00
40	81,82	0,00	18,18	0,00
41	63,64	0,00	36,36	0,00
42	100,00	0,00	0,00	0,00
43	81,82	0,00	18,18	0,00
44	81,82	0,00	18,18	0,00

N. R. = not relevant

11 participating institutions

Lund University Library - Bibliothèque nationale de France, Paris - British Library, London - National Library of Norway - National Library of Ireland, Dublin - National Széchényi Library of Hungary - Koninklijke Bibliotheek van België / Bibliothèque royale de Belgique, Brussels - Bayerische Staatsbibliothek, München - Koninklijke Bibliotheek, The Hague - Uppsala University Library - Royal Danish Library

Access & Use	yes	no	in part	N. R.
45	100,00	0,00	0,00	0,00
46	90,91	0,00	9,09	0,00
47	100,00	0,00	0,00	0,00
48	100,00	0,00	0,00	0,00
49	36,36	54,55	9,09	0,00
50	45,45	9,09	45,45	0,00
51	90,91	0,00	9,09	0,00
52	100,00	0,00	0,00	0,00
53	45,45	9,09	45,45	0,00
54	9,09	45,45	36,36	9,09
55	90,91	0,00	9,09	0,00
56	45,45	0,00	45,45	9,09
57	100,00	0,00	0,00	0,00
58	100,00	0,00	0,00	0,00
59	100,00	0,00	0,00	0,00
60	90,91	0,00	9,09	0,00
61	81,82	0,00	18,18	0,00
62	100,00	0,00	0,00	0,00
63	27,27	27,27	27,27	18,18
64	63,64	9,09	0,00	27,27
65	54,55	9,09	27,27	9,09
66	27,27	27,27	45,45	0,00
67	45,45	9,09	45,45	0,00
68	36,36	9,09	54,55	0,00
69	9,09	54,55	36,36	0,00
70	72,73	9,09	18,18	0,00
71	36,36	27,27	36,36	0,00
72	36,36	45,45	9,09	9,09
73	81,82	9,09	9,09	0,00
74	54,55	9,09	18,18	18,18

Exhibition & Transport	yes	no	in part	N. R.
75	90,91	0,00	9,09	0,00
76	81,82	0,00	18,18	0,00
77	63,64	9,09	27,27	0,00
78	90,91	0,00	9,09	0,00
79	54,55	18,18	27,27	0,00
80	90,91	0,00	9,09	0,00
81	45,45	9,09	36,36	9,09
82	100,00	0,00	0,00	0,00
83	100,00	0,00	0,00	0,00
84	90,91	0,00	9,09	0,00
85	100,00	0,00	0,00	0,00
86	90,91	9,09	0,00	0,00
87	54,55	9,09	36,36	0,00
88	36,36	0,00	54,55	9,09
89	72,73	9,09	18,18	0,00
90	81,82	9,09	0,00	9,09

Unusual & Crisis	yes	no	in part	N. R.
91	90,91	0,00	9,09	0,00
92	36,36	0,00	63,64	0,00
93	81,82	9,09	9,09	0,00
94	45,45	18,18	36,36	0,00
95	45,45	27,27	27,27	0,00
96	45,45	18,18	36,36	0,00