CAT SCAN:
WHAT YOU NEED TO KNOW ABOUT THE FFIEC’S CYBERSECURITY ASSESSMENT TOOL
SECTION I: INTRODUCTION

TODAY, IT’S A GUIDELINE. TOMORROW, IT MAY BE AN OBLIGATION.

You might be confused as to what the regulatory bodies expect from your financial institution in terms of cybersecurity: what obligations do you have? What measures should you take? And how, exactly, will you be measured for compliance?

If so, you are not alone. In fact, the regulators themselves have shared much of your confusion and to date, have lacked any single set of standards that might be construed as a constructive guideline for cybersecurity.

To fill the gap, the Federal Financial Institutions Examinations Council (FFIEC), a group that defines itself as “a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions” by regulators including the FRB, FDIC, NCUA and the OCC, has prepared a formal guideline called the “Cybersecurity Assessment Tool” or “CAT.”

A pioneering document that is the first of its kind for cybersecurity, CAT serves two fundamental roles:

1. It offers a consistent set of standards for the various regulatory bodies, and a way for them to objectively measure and assess the cybersecurity preparedness of the institutions within their jurisdiction.

2. It gives financial institutions insight into regulatory expectations. According to the FFIEC’s website, “The Assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.”

“Experts seem to agree that it’s only a matter of time before information security is mandated by law. Over the past few years, various incarnations of bills have been proposed. While security chiefs understand the scrutiny, they have concerns about security becoming a compliance burden. They worry that this will cause businesses to lose sight of what really matters: focusing on their strategy and thinking about next threats.” —PWC

A WORD TO THE WISE—THE THIRD ROLE OF CAT

Right now, the Assessment is just that—an “assessment” without the force of law or demand for conformance. But we can learn from history: all too often, today’s “guidelines” have a way of becoming tomorrow’s obligations. Remember, for example, the OCC’s approach to managing third-party risk; what began in 2013 as a set of guidelines eventually became formal standards financial institutions must meet.

From the standpoint of sound practices, the Cybersecurity Assessment Tool makes good sense. But we advise you to go further, to treat CAT as an opportunity to assess and improve your cybersecurity status now, and to prepare yourself for the regulatory demands that will almost certainly come in the near future.

Consider this paper as a tool for the tool, a way to understand, apply and learn from CAT. In CAT Scan, you’ll gain a deeper understanding of what CAT is and how to use it, and discover a practical way to meet coming cybersecurity obligations that works seamlessly—and painlessly—with the practices you have already established.

SECTION II: WHAT IS CAT?

WHAT’S IN THE CYBERSECURITY ASSESSMENT TOOL?

Piloted in 2014 and released in June, 2015, the Cybersecurity Assessment Tool reflects the FFIEC’s recognition that “cyber incidents can have financial, operational, legal, and reputational impact,” and that as a consequence, “cybersecurity needs to be integrated throughout an institution as part of enterprise-wide governance processes, information security, business continuity, and third-party risk management.”
CAT has three parts:

I. A User’s Guide that articulates its purpose, its features, and general guidance regarding why, how, and when the tool should be applied

II. The Inherent Risk Profile, a framework for identifying risks and assessing their relative risk level, on a scale from “least” to “most,” across a wide range of potential exposures in five categories:
   1. Technologies and Connection Types
   2. Delivery Channels
   3. Online/Mobile Products and Technology Services
   4. Organizational Characteristics
   5. External Threats

III. Cybersecurity Maturity, a tool for assessing the relative quality of your risk controls and practices within a maturity spectrum that ranges from “baseline” to “innovative,” in five domains:
   1. Cyber Risk Management and Oversight
   2. Threat Intelligence and Collaboration
   3. Cybersecurity Controls
   4. External Dependency Management
   5. Cyber Incident Management and Resilience

WHAT CAT DOES

On one level, CAT equips examiners with an assessment tool consistent with the FFIEC Information Technology Examination Handbook (IT Handbook) and the NIST Cybersecurity Framework. For regulators, CAT creates a reasonably objective, standardized way to approach cybersecurity oversight.

For you, CAT provides a priceless window into regulatory expectations: what they see as risks, and what they want to see as evidence of control. For the first time, the nebulous ambition of “cybersecurity defense” has defined contours and clearly articulated goals.
Fulfilling the CAT matrices for inherent risk and maturity can give your institution practical insight in two areas:

- **Risk Grade**: By completing the Inherent Risk Profile in particular, you get a risk grade in each potentially vulnerable security area that reveals the way examiners are likely to see your relative risk exposure. You might disagree with their opinions—but at least you'll able to anticipate what they're likely to be.

- **Gap Analysis**: To increase your level of cybersecurity maturity, you'll need to implement changes and monitor their progress over time. The process begins, however, with a gap analysis—an identification of missing controls and processes that the Cybersecurity Maturity tool will help you create.

Feeling blue? You should be. By overlaying inherent risk (horizontal axis) with maturity level (vertical axis), you can anticipate what examiners expect from you. In areas of Least or Minimal risk, they’ll probably be content to see a Baseline or Evolving maturity level from your institution. But where they see Significant or Most risk, you will be required to demonstrate Advanced or even Innovative maturity. (Source: FFIEC Cybersecurity Assessment Tool User’s Guide)
WHAT CAT DOES NOT DO

For all its virtues, and the clarity of its User’s Guide, there are two important things CAT does not address—and that you definitely need to determine:

Which risks matter?
Between the Inherent Risk Profile and Cybersecurity Maturity, there are approximately 300 items to assess. But of those 300, perhaps only 200 apply to your firm; if you don’t offer merchant services, for example, the items regarding card processor activity will not apply. It’s up to you to review the entire CAT and decide what does, and does not, apply to your institution.

And what do you do about them?
CAT may give you a clear picture of what you need to do, but it doesn’t tell you how. What controls do you need to elevate your maturity? How do you implement them? How will you monitor, measure, and modify them over time? This is the difficult, bare knuckles work of cybersecurity risk management—and here, CAT alone cannot help you.

SECTION III: WHAT TO DO ABOUT CAT

HOW TO MEET CAT DEMANDS

By the FFIEC’s own admission, “This process [CAT] is intended to complement, not replace, an institution’s risk management process.” Meeting the obligations surfaced by CAT, therefore, is not a matter of creating new systems, but of integrating the examiners’ requirements into your overall risk management workflow.
You have two CAT goals:

1. To reduce the amount of work that may be imposed by examiner expectations;

2. To increase the velocity of regulatory approval; the faster they can see and approve your processes, the less their impact on your institution.

CAUTION: MANUAL LABOR WON’T MEET THE NEED

Under ordinary circumstances, managing risk through manual documentation—that is, spreadsheets—is a bad idea. But now that the examiners have formalized their intentions and revealed their expectations, manual risk management workflows have gone from bad to worse. Here’s why:

- **Silos vs. integration**: Crucial information remains distributed among many spreadsheets, across multiple functions, that need to be reconciled in order to use CAT.

- **Historical vs. real-time**: You need up to date data, not aging information. Spreadsheets limit you to historical references, not current status.

- **Slow vs. fast**: Remember, you want to increase velocity; manual processes decrease it.

- **Repetitious vs. repeatable**: When you work with manual inputs, you can be sure you’ll be working with them again. And again. Your objective: create repeatable processes that run automatically.
KEY: AUTOMATE YOUR RISK MANAGEMENT PROCESSES

To reduce work and increase velocity, automation is the key. When you move from manual spreadsheets to automated solutions, you make CAT, and your means for meeting its expectations, a regular and repeatable part of your existing risk management workflow. Here’s how:

Step 1) Integrate CAT questions into standard framework
To understand your current status, as the examiners will see it, you need to apply the Cybersecurity Assessment Tool to your institution.

ProcessUnity Risk Suite has already incorporated CAT’s risk profile inquiries and maturity standards into its risk workflow, eliminating the need to apply an additional set of external assessments to your security monitoring process.

ProcessUnity includes CAT’s inherent risk assessments into its automated risk management workflow.
Step 2) Identify the gaps
Where are the missing pieces between the risks you face and the controls you place? Smart automated tools eliminate the guesswork—and reduce human error—by automatically alerting you to risk areas that need attention.

Automation helps you identify the gaps between the potential risks you have and the controls you need in order to improve your cybersecurity maturity.

Step 3) Map risks and controls
You need to document, monitor, and manage the links between possible risks and active controls. Risk Suite not only maintains the connections, but gives you a dashboard that instantly exposes the efficacy of your controls, alerting you to areas that may require more attention.
At a glance, you and your risk management colleagues can see which controls are in place (or not!) and which are effective or ineffective.

**Step 4) Generate scorecards**

Ultimately, the examiners want evidence of your cybersecurity status and maturity. Manually, this process can take weeks. But with automation, creating scorecards that document compliance takes mere moments.

Documentation? Just choose a report and weeks of work are reduced to seconds, time and time again.
SECTION IV: CONCLUSION

ARE YOU READY FOR CAT?

The Cybersecurity Assessment Tool is not just a guideline for determining risks and evaluating controls; it is a clear window onto regulatory expectations that may soon become compliance obligations.

Are you prepared for CAT? Take a few moments to consider the following questions. If you’re not confident you can affirmatively address each issue, it may be time to talk to an IT risk management expert.

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
<th>Maybe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Have you identified all the potential cybersecurity risks CAT is targeting?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your assessment of relative risk consistent with CAT’s—and with regulatory expectations?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you know your level of cybersecurity maturity?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can you identify which risks require greater maturity?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you know the gaps in your controls and processes?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can you map your risks to your controls?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you have an automated means for monitoring and managing your risks and controls?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is your risk management workflow integrated across all functions and locations?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can you document your status with scorecards you can produce instantly?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Automation is the true key to demonstrable cybersecurity health. To learn more about effective, efficient risk management across your entire enterprise, talk to a ProcessUnity cybersecurity expert today.
ABOUT PROCESSUNITY

ProcessUnity is a leading provider of cloud-based applications for risk management and service delivery management. The company’s software as a service (SaaS) platform gives organizations the control to assess, measure, and mitigate risk and to ensure the optimal performance of key business processes. For public companies and regulated industries, ProcessUnity Risk Suite delivers effective governance and control, vendor risk mitigation, and regulatory compliance. For benefit plan administrators and other financial service firms, ProcessUnity Service Delivery Risk Management (SDRM) controls complex product offerings and strengthens client service experience. ProcessUnity is used by the world’s leading financial service firms and commercial enterprises. The company is headquartered outside Boston, Massachusetts and is funded by private investors.

HEADQUARTERS
33 Bradford Street
Concord, MA 01742
PHONE: 978-451-7655

© 2015 ProcessUnity, Inc. All Rights Reserved | www.processunity.com