

Pilots, Surgeons and Developers

Improving Application Security With Checklists



<https://www.flickr.com/photos/28476480@N04/3931491307>



© clement.127

<https://www.flickr.com/photos/57763385@N03/11354819183>



<https://www.flickr.com/photos/82993642@N03/7642566944>



- ★ Product Security Engineer
@ Salesforce
- ★ Technical Speaker
- ★ Developer, data integration,
analytics and development
processes
- ★ Techbash Conference
- ★ Potions professor
- ★ @jkuemerle /
www.kuemerle.com

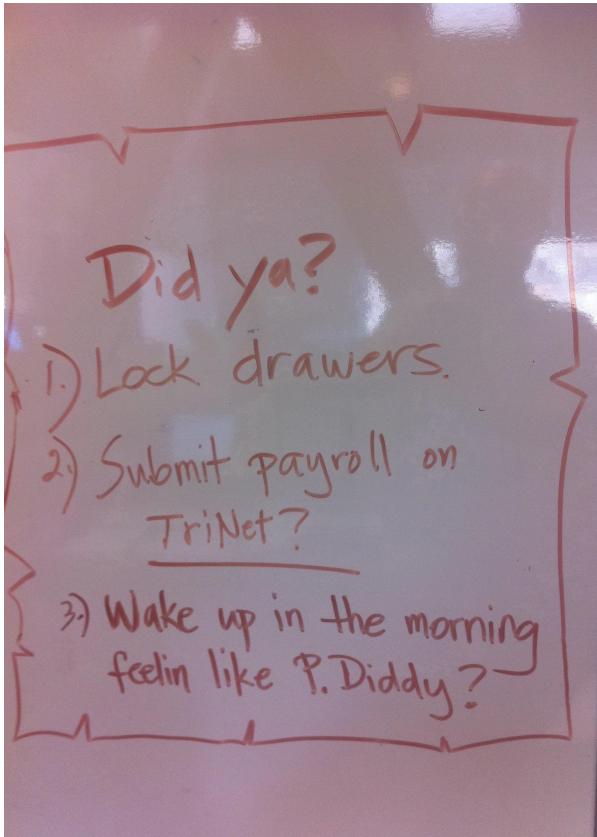
“ ...the volume of what we know has exceeded our individual ability to deliver its benefits correctly, safely, or reliably. Knowledge has both saved us and burdened us.

That means that we need a different strategy for overcoming failure, one that builds on experience and takes advantage of the knowledge people have but somehow also makes up for our inevitable human inadequacies. And there is such a strategy - though it will seem almost ridiculous in its simplicity, maybe even crazy to those of us who have spent years carefully developing ever more advanced skills and technologies.

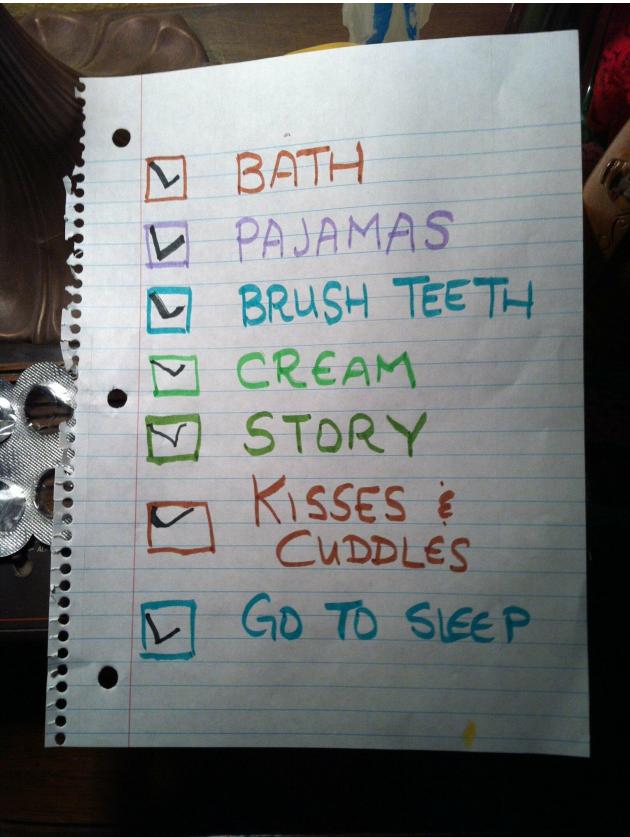
It is a checklist.”

Atul Gwande - The Checklist Manifesto

@jkuemerle



<https://www.flickr.com/photos/89306448@N00/5331464979>



<https://www.flickr.com/photos/30963564@N00/8443668738>



<https://www.flickr.com/photos/65097875@N07/7381685460>

@jkuemerle



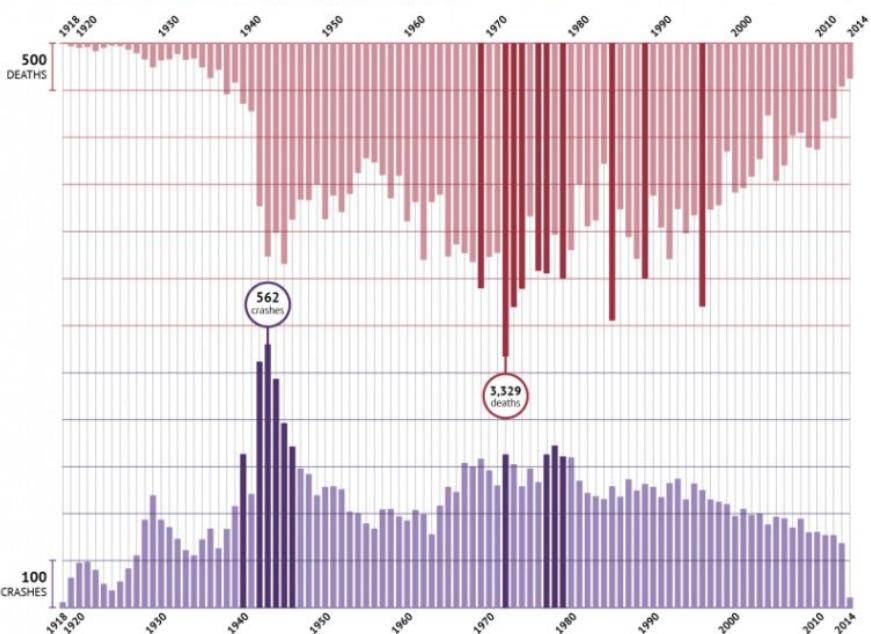
https://upload.wikimedia.org/wikipedia/commons/b/f/Harry_Potter_1st_Edition_set_stacked_with_ruler_horizontal.JPG



AVIATION ACCIDENTS AND INCIDENTS

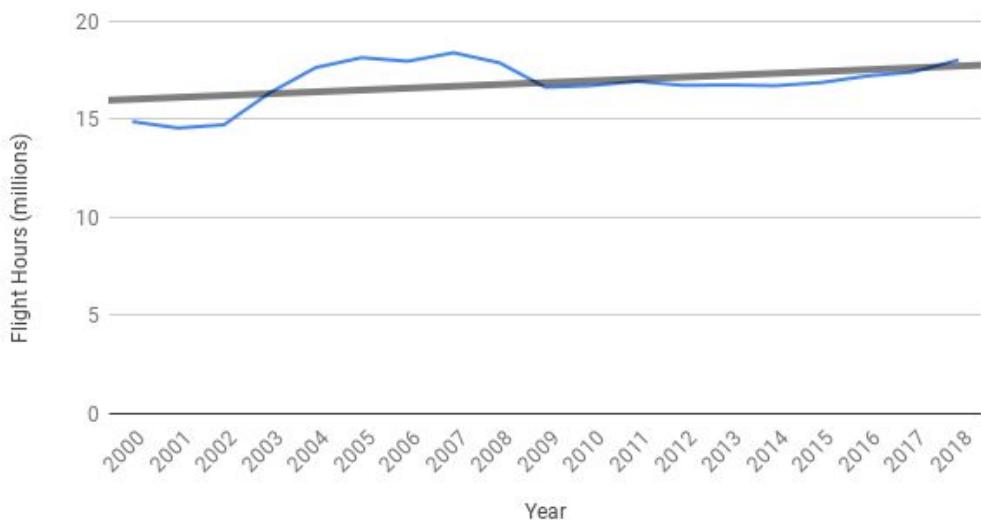
PASSENGER & CREW DEATHS, BY YEAR (TOP)

PLANE CRASHES, BY YEAR (BOTTOM)



By Lisa Mahapatra for International Business Times; Data Source: Bureau of Aircraft Accidents Archives, Geneva

United States Flight Hours



<https://www.transtats.bts.gov/TRAFFIC/>

Lessons We Can Learn From Aviation Checklists

<https://blog.safetyculture.com/checklist-best-practices/lessons-we-can-learn-from-aviation-checklists>

“Use of the WHO Surgery Checklist reduced the rate of deaths and surgical complications by more than one-third across all eight pilot hospitals.

The rate of major inpatient complications dropped from 11% to 7%, and the inpatient death rate following major operations fell from 1.5% to 0.8%.”

A surgical safety checklist to reduce morbidity and mortality in a global population

New England Journal of Medicine 2009

Surgical Safety Checklist



Patient Safety

A World Alliance for Safer Health Care

Before induction of anaesthesia

(with at least nurse and anaesthetist)

Has the patient confirmed his/her identity, site, procedure, and consent?

- Yes

Is the site marked?

- Yes
- Not applicable

Is the anaesthesia machine and medication check complete?

- Yes

Is the pulse oximeter on the patient and functioning?

- Yes

Does the patient have a:

Known allergy?

- No
- Yes

Difficult airway or aspiration risk?

- No
- Yes, and equipment/assistance available

Risk of >500ml blood loss (7ml/kg in children)?

- No
- Yes, and two IVs/central access and fluids planned

Before skin incision

(with nurse, anaesthetist and surgeon)

Confirm all team members have introduced themselves by name and role.

Confirm the patient's name, procedure, and where the incision will be made.

Has antibiotic prophylaxis been given within the last 60 minutes?

- Yes
- Not applicable

Anticipated Critical Events

To Surgeon:

- What are the critical or non-routine steps?
- How long will the case take?
- What is the anticipated blood loss?

To Anaesthetist:

- Are there any patient-specific concerns?

To Nursing Team:

- Has sterility (including indicator results) been confirmed?
- Are there equipment issues or any concerns?

Is essential imaging displayed?

- Yes
- Not applicable

Before patient leaves operating room

(with nurse, anaesthetist and surgeon)

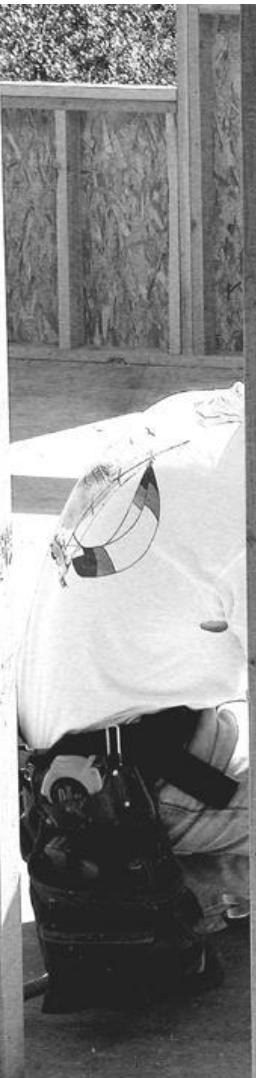
Nurse Verbally Confirms:

- The name of the procedure
- Completion of instrument, sponge and needle counts
- Specimen labelling (read specimen labels aloud, including patient name)
- Whether there are any equipment problems to be addressed

To Surgeon, Anaesthetist and Nurse:

- What are the key concerns for recovery and management of this patient?

<https://www.flickr.com/photos/21597369@N06/2091577071>



@jkuemerle

PLEASE DO NOT:

- CLIMB TOP TROLLEY
- THROW GRAVEL
- EAT GRAVEL

THANKS
M. S. T. N.
OBG

"We believe that normal checklists are intended to achieve the following objectives:

1. Provide a standard foundation for verifying aircraft configuration that will attempt to defeat any reduction in the flight crew's psychological and physical condition.
2. Provide a sequential framework to meet internal and external cockpit operational requirements.
3. Allow mutual supervision (cross checking) among crew members.
4. Dictate the duties of each crew member in order to facilitate optimum crew coordination as well as logical distribution of cockpit workload.
5. Enhance a team concept for configuring the plane by keeping all crew members "in the loop."
6. Serve as a quality control tool by flight management and government regulators over the flight crews.

Another objective of an effective checklist, often overlooked, is the promotion of a positive "attitude" toward the use of this procedure. For this to occur, the checklist must be well grounded within the "present day" operational environment, so that the flight crews will have a sound realization of its importance, and not regard it as a nuisance task (Nagano, 1975). "

Cockpit Checklists: Concepts, Design, and Use
<https://ti.arc.nasa.gov/m/profile/adegani/Cockpit%20Checklists.pdf>



@jkuemerle





<https://www.flickr.com/photos/33104187@N04/19405783446>

aviamarkin@gmail.com

@jkuemerle



aleksandrmarkin@geg
@jkuehne

“The various ways of conducting a checklist are influenced not only by the checklist device and the method of using it, but also by its “philosophy of use.” This philosophy varies among airframe manufacturers, officials of regulatory agencies, and airlines. In most cases, the checklist philosophy of use is the outgrowth of the company’s corporate culture.

...

The airline’s culture is an important factor because it is mirrored in the manner in which flight management and training departments establish, direct, and oversee flight operations and related procedures (Degani and Wiener, 1991). ”

Cockpit Checklists: Concepts, Design, and Use
<https://ti.arc.nasa.gov/m/profile/adegani/Cockpit%20Checklists.pdf>

2 \$ vi ~ / bin/a.pl

```
#!/usr/bin/perl -w
use strict;
use DBI;
use DBD::MySQL;
my $sth;
my $template; //
```



**NOT ALLOWED THROUGH
SECURITY CHECKPOINT**

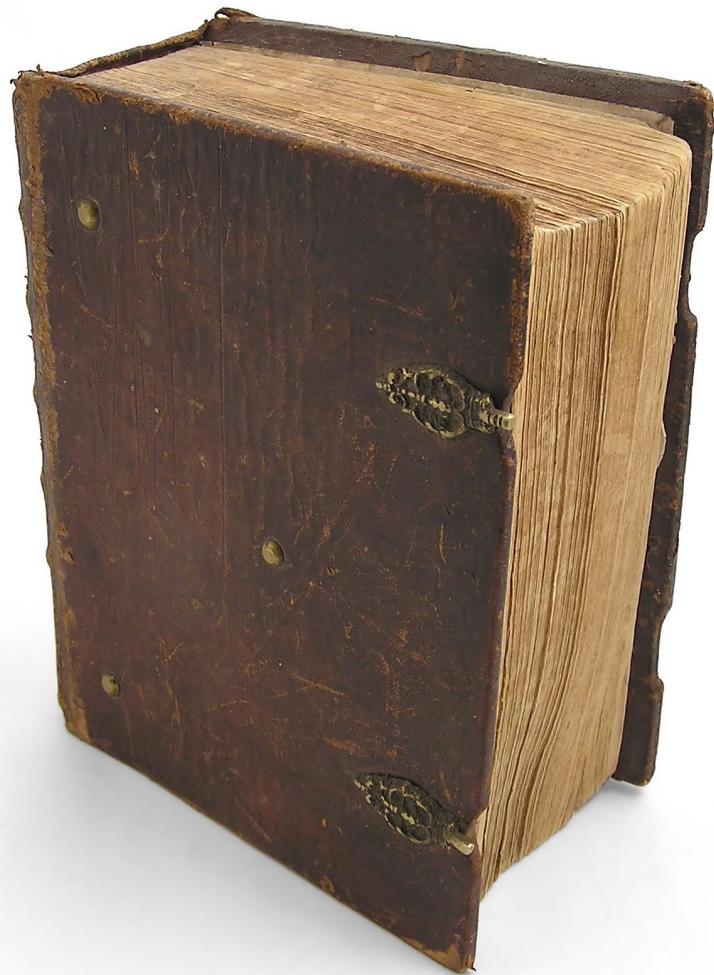


**CONTACT YOUR AIR
REPRESENTATIVE**

“Management pressure for “on-time performance” is one factor that yields high operating efficiency. Air transports fly in and out of hubs with fast turnarounds. The Department of Transportation monitors flight schedules in order to publish the highest and lowest ranking airlines in “on-time performance,” placing another public relations burden on management. Such production pressures ultimately migrate into the cockpit, and consequently affect checklist management.

The checklist procedure is highly susceptible to production pressures. These pressures lay the foundation for errors by encouraging sub-standard performance when the crew is rushing to complete the checklist in order to depart on time. Furthermore, under production pressures, checklists are sometimes “...relegated to second place status in order to save time” (Majikas, 1989). ”

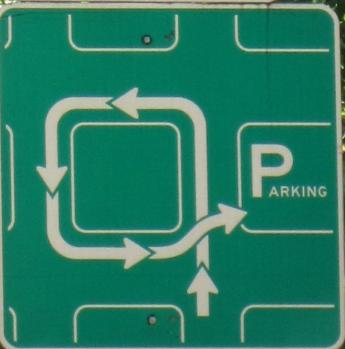
Cockpit Checklists: Concepts, Design, and Use
<https://ti.arc.nasa.gov/m/profile/adegani/Cockpit%20Checklists.pdf>



<https://www.flickr.com/photos/37914686@N00/2928818748>

@jkuemerle

<https://www.flickr.com/photos/849987970@N00/8736519237>



@jkueblerle

Version
2.0

What the Plus!

Google+ for the Rest of Us



Guy Kawasaki

BESTSELLING AUTHOR OF ENCHANTMENT



<https://www.flickr.com/photos/13998657@N02/18526571452>

@jkuemerle







Bill Sempf
@sempf

Following



QA Engineer walks into a bar. Orders a beer.
Orders 0 beers. Orders 999999999 beers.
Orders a lizard. Orders -1 beers. Orders a
sfdeljknesv.

1:56 PM - 23 Sep 2014

<https://twitter.com/sempf/status/514473420277694465>

soma fm

GATE, SAT
~~INFO~~
AND SOFTWARE



Be your own security

The world is an increasingly dangerous place. Research has shown that people need to get inspected to feel secure, even if the actual inspection is a complete farce. Yet as a society we cannot hire half the population to perform bogus inspections on the other half in order to keep up with market demand for perceived security.

What The Hack proudly introduces a new concept to the security inspection marketplace:

Do-It-Yourself Security Inspection

Unlike traditional old-style security inspections, DIY inspections are optional. This ensures no inspection effort is wasted on those that already feel secure. If you need to be inspected in order to feel safe, please proceed to perform the by-now familiar security procedures on yourself. Should you feel unsafe again at any time during the event, then please feel free to re-inspect yourself and/or your belongings here as often as you feel is needed.

When was the last time you were inspected by someone as smart as you?
With our patented ***inherent adaptive inspection intelligence technology***
the terrorists don't stand a chance.

Please take a moment to ask yourself
the following questions:

1. Did anyone help you pack your luggage?
2. Were you with your luggage at all times?
3. Did anyone give you any items to take to this event?
4. Where did you book your ticket?
5. How did you pay for this event?
6. What is the purpose of your visit?
7. Where will you be staying?

Have a nice day!

Am I allowing the user to change the value of stored data?

- No
- Yes, and I am making sure the user is both identified and is authorized to make the requested changes

Am I exposing an internal identifier value to the user?

- No
- Yes, and I am making sure the user is both identified and is authorized to view or work with the item

Am I returning any values that the user entered back to the user?

- No
- Yes, and I am making sure the values are escaped for the rendering context

Am I processing any user provided XML data?

- No
- Yes, and I am using an XML parser that is configured to reject embedded document type declarations (DTD)

1. Checklist responses should portray the desired status or the value of the item being considered, not just “checked” or “done.”

Items all have status indicating desired value

2. A long checklist should be subdivided to smaller task-checklists or chunks that can be associated with systems and functional areas.

Checklist is subdivided according to task specific areas

3. Sequencing of checklist items should follow a meaningful organization of the tasks, and be performed in a logical flow.

Checklist items are in a logical order

4. Checklist items should be sequenced in parallel with internal and external activities that require input from other parties (operations, project/product management, stakeholders)

Items that require external input are in parallel

5. The most critical items on the task-checklist should be listed as close as possible to the beginning of the task-checklist, in order to increase the likelihood of completing the item before interruptions may occur. This could conflict with No. 4 above. In most cases where this occurs, this guideline (No. 5) should take precedence.

Critical items are listed as close as possible to the top

6. Critical checklist items that might need to be reevaluated due to new information (modified by items occurring after an initial check), should be duplicated in checklists for the appropriate situation (testing, runtime, etc.).

Items requiring reevaluation are duplicated where appropriate

7. The completion call of a checklist should be written as the last item on the checklist, allowing all team members to move mentally from the checklist to other activities with the assurance that the checklist has been completed.

Checklist ends with a completion task

8. Critical checklists should be completed early in the process in order to decouple them from the other activities that may cause distraction.

Critical checklist is documented to be completed first

9. Checklists should be designed in such a way that their execution will not be tightly coupled with other tasks. Provide buffers for recovery from failure and a way to “take up the slack” if checklist completion does not keep pace with the external and internal activities.

Checklists do not have tightly coupled tasks

10. Teams should be aware that the checklist procedure is highly susceptible to production pressures. These pressures set the stage for errors by possibly encouraging substandard performance, and may lead some to relegate checklist procedures to a second level of importance, or not use them at all.

Development has a sense of ownership of checklists



What
would
Tony
Stark
do?

References

- The Checklist Manifesto - Atul Gawande <http://bit.ly/ChecklistManifestoOWASP>
- Hidden Brain Podcast: You 2.0: Check Yourself <http://bit.ly/HiddenBrainChecklist>
- Cockpit Checklists: Concepts, Design, and Use <http://bit.ly/CockpitChecklistOWASP>
- Human Factors of Flight-Deck Checklists: The Normal Checklist
<http://bit.ly/HumanFactorsChecklists>
- A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population (NEJM) <http://bit.ly/SurgicalSafetyStudy>
- Safe Surgery (WHO) <https://www.who.int/patientsafety/safesurgery/en/>



Joe Kuemerle - @jkuemerle
<https://github.com/jkuemerle/OWASP-DC-2019>